

https://dspace.org/

# Arithmetic in the ring of Gaussian integers

**Molelekeng, Beverly**

**2022**

https://hdl.handle.net/10539/33915

Downloaded from a DSpace repository. https://dspace.org/

UNIVERSITY OF THE WITWATERSRAND
JOHANNESBURG

SCHOOL OF MATHEMATICS

# ARITHMETIC IN THE RING OF GAUSSIAN INTEGERS

*Author:*

BEVERLY MOLELEKENG

*Supervisor:*

Prof A. O MUNAGI



# Declaration

I hereby declare that the project report titled "ARITHMETIC IN THE RING OF GAUSSIAN INTEGERS" submitted to the university of the Witwatersrand under the School of Mathematics, is based on the work I carried out during the course of the year under the supervision of Prof A.O Munagi.

Signature: $B.T.Molelekeng$

Date: $14 - February - 2022$

# Dedication

To my mother, the epitome of beauty, resilience, and grace. Thank you for all you do for me. For the constant support and countless sacrifices, you truly are a remarkable woman, a true woman of influence. I will forever be in awe of the part you continue to play in making sure that every dream of mine is attainable, and most of the time, successful. Thank you very much. To the rest of my family for always lending an ear and a helping hand at times of need, I thank you all. You have filled my journey with love, hope and adventure. I will forever be indebted to each and every single one of you for your noble acts of selflessness where I am concerned. To my supervisor for his patience and guidance. Thank you for walking this road with me. Words can never express just how grateful I am.

# Abstract

We study the ring of integers $\mathbb{Z}$, and use it's properties along with those of complex numbers to explore the nature of the ring of Gaussian integers $\mathbb{Z}[i]$. We introduce an analogue of the key concepts of the ring $\mathbb{Z}$ in $\mathbb{Z}[i]$ such as factorization and modular arithmetic. One approach is by mimicking the statements and proofs in $\mathbb{Z}$ and modifying them to accommodate the 2-dimensional aspect of the elements of $\mathbb{Z}[i]$. Then we investigate ways of extending this information to general quadratic rings of the form $\mathbb{Z}[\sqrt{d}]$, where $d$ is a square-free integer.

# Contents

**Declaration** **1**

**Dedication** **2**

**Abstract** **2**

**1 Introduction** **7**
1.1 Background and Preliminaries . . . . . 8

**2 Properties of $\mathbb{Z}[i]$** **10**
2.1 The Norm Function . . . . . 12
2.2 Units . . . . . 14
2.3 Integral Domains . . . . . 16
2.4 Euclidean Domains . . . . . 18

**3 Divisibility and The Euclidean Algorithm** **22**
3.1 Divisibility Properties and Ideals . . . . . 22
3.2 Gaussian Integer Division . . . . . 29

**4 Factorization** **37**
4.1 Factorization in $\mathbb{Z}$ . . . . . 37
4.2 Gaussian Integer Factorization . . . . . 40
4.3 When Unique Factorization Fails . . . . . 45
4.4 Recovering Unique Factorization . . . . . 48

**5 Modular Arithmetic In $\mathbb{Z}[i]$** **50**
5.1 Modular Arithmetic in $\mathbb{Z}$ . . . . . 50
5.1.1 Factor Groups/Residue Classes . . . . . 52
5.2 Utilizing Modular Arithmetic in $\mathbb{Z}[i]$ . . . . . 54

5.3 Modular Arithmetic on Squares . . . . . 58
5.3.1 Modular Arithmetic on Irreducible Polynomials . . . . . 59

**6 Gaussian Primes** **62**
6.1 Pure Gaussian Primes . . . . . 62
6.2 Gaussian Integer primes of the form a+bi, a=0 and b=0 . . . . . 63

**7 Application** **68**
7.1 General Application . . . . . 68
7.2 Pythagorean Triples . . . . . 71

**8 Conclusion** **75**

**bibliography** **77**

# List of Tables

2.1 Unit Table . . . . . 15

4.1 Gaussian Integer Factorization Table . . . . . 46

5.1 Reduction Table For 11 . . . . . 59

# Chapter 1

# Introduction

The German mathematician Carl Friedrich Gauss (1777-1855) proved that a ring of integers R in the quadratic field $\mathbb{Q}[\sqrt{d}]$ is a unique factorization domain or (UFD) if $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ [2, 19] . The German mathematician Ernst Kummer (1810-1893) studied the rings where unique factorization fails and made significant contributions to the theory of ideals. Kummer argued that the integers of a number field must be embedded into a domain of ideal numbers that is bigger, and where the unique factorization of ideals into prime ideal numbers is possible [20]. However, the German mathematician Richard Dedekind (1831-1916) is credited for formulating the modern foundations of algebraic number theory which he achieved by providing the correct definition of a ring of integers in a number field, and proving that an ideal can be factored uniquely into a product of prime ideals in these rings [4, 17]. Concepts like Fermat's Last Theorem, discovered by the French mathematician Pierre de Fermat (1607-1665), reciprocity laws and binary quadratic laws for example, played a huge role in the origins of algebraic number theory. This is because as most of the problems were presented in the ring $\mathbb{Z}$, solving these equations required the integers to be embedded into domains of algebraic integers [16]. We are interested in the ring of Gaussian integers. According to Milne [17], Gauss studied Gaussian integers in order to find a quartic reciprocity law in the year $1832$. This is documented in his second monograph on quartic reciprocity. Gauss used Gaussian integers to provide the first proof of the law of biquadratic reciprocity, which was earlier studied by the Swiss mathematician Leonhard Euler (1707-1783). The French mathematician Adrienne-Marie Legendre (1752-1833) also provided the proof the quadratic reciprocity law, but his proof was incomplete [17]. He also dis-

covered the Legendre symbol $\left(\frac{\alpha}{p}\right)$ which we will use with alongside concepts like Euler's criterion in the paper.

## 1.1 Background and Preliminaries

Let $K$ be a subfield of the complex numbers $\mathbb{C}$ containing the rationals $\mathbb{Q}$, that is, $\mathbb{Q} \subset K \subset \mathbb{C}$. Then $K$ is a vector space over $\mathbb{Q}$. If the dimension of $K$ is finite, $\dim_{\mathbb{Q}} K = [K, \mathbb{Q}] < \infty$, we say that $K$ is an *algebraic number field*.

Any $\alpha \in K$ is an *algebraic number*. This means that $\alpha$ is the root of a polynomial equation over $\mathbb{Q}$. Indeed if $[K, \mathbb{Q}] = n$, then the $n + 1$ elements $1, \alpha, , \alpha^2, \ldots, , \alpha^n$ are linearly dependent. Thus there exist $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ (not all zero) such that

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Examples of number fields include $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{7})$, $\mathbb{Q}(2^{1/3})$ and more generally, $\mathbb{Q}(\alpha)$ for any algebraic number $\alpha$.

Note that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

An *algebraic integer* is an algebraic number which is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

The set $\mathcal{O}_K$ of algebraic integers of a number field $K$ forms a subring of $K$. The ring $\mathcal{O}_K$ is called the ring of integers of $K$.

For example, if $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$, and if $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$, etc.

For this research, we will focus on the ring of integers of

$$K = \mathbb{Q}[i] = \mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} | a, b \in \mathbb{Q}\},$$

namely

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}.$$

We will study the properties of this ring using the ring of integers $\mathbb{Z}$, as a point of reference. This strategy is justifiable since integers, which we sometimes call ordinary integers are Gaussian integers from the definition of Gaussian integers. To connect these two rings we use the norm map $N : \mathbb{Z}[i] \mapsto \mathbb{Z}$, defined by $N(a + bi) = a^2 + b^2$, which is an instance of the map

$$\varphi : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}, \text{ defined by } \varphi(a + b\sqrt{d}) = |a^2 - b^2 d|.$$

We want to prove that not only is $\mathbb{Z}[i]$ a ring, it is a subring of the complex numbers, and as a result we can assign every Gaussian integer an inverse that lies in $\mathbb{C}$, and prove that $\mathbb{Z}[i]$ is an integral domain, since we can use concepts like the cancellation law to counter any formation of zero divisors. We then want to use the norm map to show that $\mathbb{Z}[i]$ is a Euclidean domain, which implies that it is a principal ideal domain (PID), and as such we can introduce concepts such as the division algorithm, the Euclidean algorithm, and consequently, greatest common divisors. From understanding how division operates in $\mathbb{Z}[i]$ we want to use the knowledge to show that $\mathbb{Z}[i]$ is a unique factorization domain. This can be proven using the multiplicative property of the norm $N : \mathbb{Z}[i] \mapsto \mathbb{Z}$, and that when the Gaussian integer $a+bi$ is nonzero, the norm is a natural number, hence the factorization has to terminate at some point since the ring $\mathbb{N}$ is well-ordered. This is an attempt to mimic the fundamental theorem of arithmetic for $\mathbb{Z}$ which states that every nonzero integer $\alpha > 1$, can be factored into a product of primes in $\mathbb{Z}$, and that said factorization is unique. This classic theorem introduces elements called irreducible and reducible elements in $\mathbb{Z}$, which are basically primes and non-primes in $\mathbb{Z}$. We want to introduce an analogue of this theorem in $\mathbb{Z}[i]$ so that we can discuss the nature of Gaussian integer factorization, and what the irreducible and reducible elements in $\mathbb{Z}[i]$ are. With this in mind, we can explore the concept of the uniqueness of factorization. The premise of unique factorization is the belief that every element in a unique factorization domain $R$ can be factored uniquely into a product of the irreducibles of $R$, up to order of units and associates, and depending on the ring we are operating in, irreducible elements have close links to prime elements in that ring. Using this information we want to prove that $\mathbb{Z}[i]$ is a unique factorization domain, and hence we can form theorems connecting Gaussian irreducibles to Gaussian primes. We then introduce equivalence relations and partitions on a set to explore modular arithmetic in $\mathbb{Z}$, which plays a major role in the formation of factor rings. We use factor rings to further explore previous concepts like what happens when a ring is not an integral domain. Lastly, we will use all the information to study the various types of Gaussian primes, starting with primes that are considered to be pure Gaussian integer primes, which are just pure Gaussian integers $a+bi$ where $a, b \neq 0$, and $N(a+bi) = p$, for a prime $p \in \mathbb{N}$, to Gaussian primes $p = 4k+1$, that can be expressed as a sum of two squares, and the Gaussian primes of the form $p = 4k+3$, that cannot be expressed as a sum of two squares. This work will assist in applying some perspective to the expression $x^2 + y^2$, from $\mathbb{Z}$ which we will factor into the linear factors $(x+yi)(x-yi)$, in $\mathbb{Z}[i]$. This way we can formulate a general method in $\mathbb{Z}[d]$ that will help us solve various equations in $\mathbb{Z}$ in an artful way.

# Chapter 2

# Properties of $\mathbb{Z}[i]$

We begin the section by defining a general ring as according to Judson [14], and use this definition to prove that $\mathbb{Z}[i]$ is a ring.

**Theorem 2.0.1.** *A ring $(R, +, \cdot)$ is a set $R$ with the binary operations $+$ (addition), and $\cdot$ (multiplication) that satisfies the following axioms for all $\alpha, \beta$ in $R$:*

- $\alpha + \beta = \beta + \alpha$.
- $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
- *There exists an element $0_R$ such that,* $\alpha + 0_R = \alpha$.
- *There exists an element $-\alpha$ in $R$ such that,* $\alpha + (-\alpha) = 0_R$.
- $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.
- *There exists an element $1_R$ such that,* $1_R \cdot \alpha = \alpha$.
- $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.

**Definition 2.0.1.** *A ring $R$ is called a commutative ring if $\alpha\beta = \beta\alpha$, for all $\alpha, \beta$ in $R$.*

**Theorem 2.0.2.** *The set $(\mathbb{Z}[i], +, \cdot)$ is a ring.*

*Proof.* Let $(a + bi), (c + di), (e + fi)$ be Gaussian integers.

- $(a + bi) + (c + di) = a + bi + c + di = (a + c) + (b + d)i \in \mathbb{Z}[i]$ (addition is well-defined)

- $(a+bi)+[(c+di)+(e+fi)] = a+bi+(c+di+e+fi) = a+bi+c+di+e+fi = [(a+bi)+(c+di)]+(e+fi) \in \mathbb{Z}[i]$ (addition is associative).
- $(a+bi)+(c+di) = a+bi+c+di = (c+di)+(a+bi) \in \mathbb{Z}[i]$ (addition commutes).
- There is an element $0_{\mathbb{Z}[i]}$ in $\mathbb{Z}[i]$ such that, $(a+bi)+0_{\mathbb{Z}[i]} = (a+bi)$, $\forall(a+bi) \in \mathbb{Z}[i]$ (additive identity).
- $\forall(a+bi) \in \mathbb{Z}[i]$, there exists an element $[-(a+bi)]$ in $\mathbb{Z}[i]$, such that $(a+bi)+[-(a+bi)] = 0_{\mathbb{Z}[i]}$
- $(a+bi)(c+di) = ac+adi+cbi+bdi^2 = (ac-bd)+(ad+cb)i \in \mathbb{Z}[i]$ (additive inverse).
- There is an element $1_{\mathbb{Z}[i]}$ such that $(a+bi)\cdot 1_{\mathbb{Z}[i]} = 1_{\mathbb{Z}[i]}\cdot(a+bi) = (a+bi), \forall(a+bi) \in \mathbb{Z}[i]$ (multiplicative identity).
- $(a+bi)\cdot[(c+di)\cdot(e+fi)] = e(ac-bd)+f(ad+cb)i = [(a+bi)\cdot(c+di)]\cdot(e+fi)$ (associative law).
- $(a+bi)\cdot[(c+di)+(e+fi)] = (ac+adi+cbi-bd)+(ae+afi+bei-bf) = [(a+bi)\cdot(c+di)]+[(a+bi)(e+fi)]$ (distributive law).

□

**Theorem 2.0.3.** *The ring $\mathbb{Z}[i]$ is a commutative ring.*

*Proof.* Let $a+bi$ and $c+di$ be Gaussian integers. Then,

$$\begin{aligned}(a+bi)(c+di) &= ac+adi+cbi+bdi^2\\ &= ca+bci+dai+dbi^2\\ &= (c+di)(a+bi).\end{aligned}$$

Therefore by Definition 2.0.1, $\mathbb{Z}[i]$ is a commutative ring. □

It is very important to note that in the ring $\mathbb{Z}[i]$, $1$ and $0$ are distinct elements. In fact the condition $1 = 0$ is only true if the ring is what we call a zero ring. By Rotman [22], some authors define rings excluding the identity element $1$. This definition accomodates the ring $2\mathbb{Z}[i]$ which is a subring of $\mathbb{Z}[i]$. For this paper, every ring contains $1$.

**Definition 2.0.2** (Trifkovic [25]). *A ring $R$ is called a zero ring if $R$ is a singleton ring where $\alpha = 0$, for $\alpha \in R$.*

**Definition 2.0.3** (Trifkovic [25]). *Let $R$ be a ring under the operations $+$ and $\cdot$. The set $S$ is called a subring of $R$, denoted by $S \subseteq R$, if for all $\alpha$ and $\beta$ in $S$ we have,*

- $1 \in S$.
- $-\alpha \in S$.
- $\alpha + \beta \in S$.
- $\alpha \cdot \beta \in S$.

Using Theorem 2.0.2, and Definition 2.0.3 , $\mathbb{Z}[i]$ satisfies all the conditions to become a subring of $\mathbb{C}$, hence $\mathbb{Z}[i]$ inherits concepts from the ring $\mathbb{C}$, that we will use to further understand Gaussian integers.

## 2.1 The Norm Function

Let $R \subseteq \mathbb{C}$ be a ring, and $z = x + yi$ be a complex number. We use Stillwell [24] to introduce the properties of conjugation in complex numbers.

**Proposition 2.1.1.** *For every complex number $z = x + yi$ in $R$, we can assign another complex number called the complex conjugate of $z$, denoted by $\overline{z} = x - yi$ satisfying the following identities,*

- $z \cdot \overline{z} = x^2 + y^2$.
- $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
- $\overline{z + w} = \overline{z} + \overline{w}$,

*for all $z$ and $w$ in $R$. Furthermore we have the map $z \to \overline{z} : \mathbb{Q}[i] \to \mathbb{Q}[i]$. We call the map $z \to \overline{z}$ an automorphism.*

Let $z = x + yi$ be a complex number. To find the magnitude of $z$ we compute the quantity

$$|z| = \sqrt{x^2 + y^2}.$$

When dealing with complex numbers, any value of $|z|$ is acceptable since $\sqrt{n} \in \mathbb{C}$ for all values of $n$, but how do we approach this concept in $\mathbb{Z}[i]$?. We want to calculate the magnitude of any Gaussian integer, but we want to restrict the magnitude to ordinary integers since they too are Gaussian integers.

**Example 1.** *Consider the Gaussian integer $z = 1 + 2i$. Then*

$$|z| = \sqrt{(1)^2 + (2)^2} = \sqrt{5},$$

*but we want to avoid any encounter with irrational numbers like this in $\mathbb{Z}[i]$. So what is the alternative?*

We can solve the problem above by computing the equation by squaring $\sqrt{5}$ to obtain the ordinary integer $5$ instead.

In general, to make sure that the magnitude of every Gaussian integer $a + bi$ is always an ordinary integer, we compute

$$|z|^2 = z\overline{z} = a^2 + b^2 = N(z). \tag{2.1}$$

We call $N(z)$ the norm of the Gaussian integer $z$.

**Theorem 2.1.2.** *Let $N$ be the norm of a Gaussian integer $z = a + bi$, then*

$$N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}.$$

*Proof.* Let $z \in \mathbb{Z}[i]$, defined by $z = a + bi$. Then by Proposition $2.2.1$ we know that $\overline{z} = a - bi$. We also have

$$z\overline{z} = a^2 + b^2.$$

Since $a, b \in \mathbb{Z}$, we have $a^2 + b^2 \in \mathbb{Z}$. If $z = 0$, then $a^2 + b^2 = 0$, and for $z \neq 0$ we have $a^2 + b^2 > 0$.

$\therefore N(a + bi) = a^2 + b^2 \in \mathbb{N} \cup \{0\}$.

□

We next check the properties that the norm function satisfies in the ring $\mathbb{Z}[i]$. For referencing purposes, we let $N : \mathbb{Z}[i] \to \mathbb{Z}$, keeping in mind that by $\mathbb{Z}$, we are referring only to $0$ and the strictly positive ordinary integers.

**Corollary 2.1.2.1.** *The function $N : \mathbb{Z}[i] \to \mathbb{Z}$, defined for all nonzero $\alpha, \beta \in \mathbb{Z}[i]$ satisfies the following conditions;*

- $N(\alpha) > 0$.

- $N(\alpha\beta) = N(\alpha)N(\beta)$.
- $N(1_{\mathbb{Z}[i]}) = 1$.

*Proof.* The proof of the first bullet point follows from the proof of Theorem 2.1.2.

- Let $\alpha = a + bi, \beta = c + di$.

$$\begin{aligned} N(\alpha\beta) &= (\alpha\beta)(\overline{\alpha\beta}) \\ &= (\alpha\overline{\alpha})(\beta\overline{\beta}) \\ &= (\alpha\beta)(\overline{\alpha}\overline{\beta}) \\ &= N(\alpha)N(\beta). \end{aligned}$$

- $N(1 + 0i) = (1)^2 + (0)^2 = 1 \in \mathbb{Z}$.

□

## 2.2 Units

We want to introduce units for a ring $R$, and the properties of these units using Trifkovic [25].

**Definition 2.2.1.** *Let $\alpha \neq 0$ in $R$. We say $\alpha$ has a multiplicative inverse in $R$ if there exists an element $\beta$ in $R$ such that $\alpha\beta = 1$.*

**Definition 2.2.2.** *A unit of $R$ is an element $\alpha \in R$ that has a multiplicative inverse in $R$. We usually denote this inverse as $\alpha^{-1}$.*

For this paper we will denote the units of the ring $R$ as $U(R)$.

**Proposition 2.2.1** (Properties of Units)**.** *Let $R$ be a ring. The following results are true.*

- *If $\alpha \in U(R)$, then $-\alpha \in U(R)$.*
- *If $\alpha \in U(R)$, then the inverse of $\alpha$ denoted by $\alpha^{-1}$ is also in $U(R)$.*
- *If $\alpha \in U(R)$, and $\beta \in U(R)$, then $\alpha\beta \in U(R)$.*

**Definition 2.2.3.** *Two elements $\alpha$ and $\beta$ in $R$ are called associates if $\alpha = u\beta$, for some $u \in U(R)$.*

We want to study units and associates when $R = \mathbb{Z}[i]$.

**Proposition 2.2.2.** *An element $u$ of $\mathbb{Z}[i]$ is a unit if and only if $N(u) = 1$.*

*Proof.* $\Rightarrow$ Let $\alpha$ be a unit of $\mathbb{Z}[i]$. By Definition 2.2.2, there exists an element $v$ in $\mathbb{Z}[i]$ such that $uv = 1$. Taking the norm of the equation we get $N(uv) = N(1)$, which gives us $N(u)N(v) = 1$. Therefore $N(u) = 1$.

$\Leftarrow$ Let $N(u) = 1$. Since $N(u) = u\overline{u}$, we have $u\overline{u} = 1$, therefore $u^{-1} = \overline{u}$ as desired.

□

**Proposition 2.2.3** (Conrad [9])**.** *The only units of $\mathbb{Z}[i]$ are the elements $1, -1, i, -i$.*

*Proof.* $\Rightarrow$ Each of the elements $1, -1, i, -i$ are invertible in $\mathbb{Z}[i]$ since $1 \cdot 1 = 1, -1 \cdot -1 = 1$, and $i \cdot -i$.

$\Leftarrow$ Let $\alpha = a + bi$ be a nonzero Gaussian integer. If $\alpha$ is a unit then by Definition 2.2.2 there exists a Gaussian integer $\beta$ such that $\alpha\beta = 1$. Taking the norm of the equation we get $N(\alpha\beta) = N(\alpha)N(\beta) = 1$. By Corollary 2.1.2.1, $N(\alpha) > 0$ since $\alpha$ is non-zero. This implies that $N(\alpha) = 1$. Since $\alpha = a + bi$, we have $N(\alpha) = a^2 + b^2$, which gives the equation $a^2 + b^2 = 1$. The solution to this equation is then $\alpha = 1, -1, i, -i$.

□

We shall denote the set of units of $\mathbb{Z}[i]$ as $U(\mathbb{Z}[i])$, and the units of a general ring as $U(R)$. The multiplication table below illustrates the proof of Proposition 2.2.3, particularly for our integral domain $\mathbb{Z}[i]$.

| Unit | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

Table 2.1: Unit Table

## 2.3 Integral Domains

For this section we use Alaca [1] to define an integral domain, and the properties of an integral domain.

**Definition 2.3.1.** *Let $R$ be a commutative ring. An element $\alpha \neq 0 \in R$ is called a zero divisor of $R$ if $\exists\ \beta \neq 0 \in R$ such that either*

1. $\alpha\beta = 0$*, i.e $\alpha$ is a left zero divisor of R.*
2. $\beta\alpha = 0$*, i.e $\alpha$ is a right zero divisor of R.*

**Definition 2.3.2.** *A commutative ring $R \neq \{0\}$ with no zero divisors is called an integral domain.*

**Definition 2.3.3.** *Let $R$ be an integral domain. If $\alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma$ for all $\alpha \neq 0$, this is called the left cancellation law.*

**Definition 2.3.4.** *Let $R$ be an integral domain. If $\alpha\gamma = \beta\gamma \Rightarrow \alpha = \beta$ for all $\gamma \neq 0$, this is called the right cancellation law.*

Combining $(1)$ and $(2)$ gives us the cancellation law.

**Theorem 2.3.1.** *Let $R$ be a commutative ring. If $R$ has the left cancellation property, then $R$ has no zero divisors, and consequently, $R$ is an integral domain.*

*Proof.* Choose some $\alpha \neq 0 \in R$. Suppose $R$ has the left cancellation property and suppose we can find some $\beta \neq 0 \in R$, such that $\alpha\beta = 0$. Then $\alpha$ is a left zero divisor of $R$. However, since $R$ has the left cancellation property, we have

$$\begin{aligned} \alpha\beta = 0 = \alpha 0 \\ \Rightarrow \beta = 0. \end{aligned}$$

$\therefore R$ has no zero divisors. This makes $R$ an integral domain by definition. $\square$

**Remark 1.** *We can use the same methodology to show that if an arbitrary commutative ring $R$ has the right cancellation property, then $R$ has no zero divisors.*

**Theorem 2.3.2.** *The ring $\mathbb{Z}[i]$ is an integral domain.*

*Proof.* We wish to show that $\mathbb{Z}[i]$ has no zero divisors. Let $a + bi$ and $m + ni$ be Gaussian integers, and suppose

$$(a + bi)(r + si) = 0.$$

Let $a + bi \neq 0$. Since $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, we know that $a + bi$ has an inverse in $\mathbb{C}$ denoted by $(a + bi)^{-1} = \dfrac{1}{a + bi}$. Multiplying by the inverse gives us

$$\begin{aligned}(a + bi)^{-1} \cdot (a + bi)(r + si) &= (a + bi)^{-1} \cdot 0 \\ \Rightarrow (1) \cdot (r + si) &= 0 \\ \Rightarrow (r + si) &= 0.\end{aligned}$$

$\therefore \mathbb{Z}[i]$ has no zero divisors, and is thus an integral domain.

□

We will see an example of what happens when a ring is not an integral domain in Chapter 5.

**Definition 2.3.5.** *We define a field $K$ to be a commutative ring with an identity element $1_K$, where every nonzero $\alpha$ in $K$ is a unit.*

**Remark 2.** *From the proof that $\mathbb{Z}[i]$ is an integral domain, we can see that every field $K$ is an integral domain, because if we have $\alpha\beta = 0$ for some $\alpha, \beta$ in $K$, then we can always introduce the inverse to make sure that one of the elements will be equal to zero.*

*Since $\mathbb{Q}[i]$ is all fraction of $\mathbb{Z}[i]$, the fraction $\dfrac{1}{a + bi}$, is contained in $\mathbb{Q}[i]$, and we call $\mathbb{Q}[i]$ the field of fractions of $\mathbb{Z}[i]$.*

Notice that in the field $K$, we did not have to worry about the condition,

$$1 = 0,$$

as we had to address in $\mathbb{Z}[i]$. This is because the multiplicative inverses of $F$ only exist when $K = K \setminus \{0\}$. This condition assures us that in a field, $1$ and $0$ are two different elements.

## 2.4 Euclidean Domains

We use Conrad [8] to introduce a Euclidean function in the integral domain $R$, that will make $R$ a Euclidean domain.

**Definition 2.4.1.** *An integral domain $R$ is called a Euclidean domain if there is a function $\phi : R - \{0\} \to \mathbb{N}$ such that:*

1. *$\phi(\alpha) \leq \phi(\alpha\beta)$ for all nonzero $\alpha, \beta$ in $R$,*
2. *For all $\alpha, \beta \in R$ with $\beta \neq 0$ we can find $q$ and $r$ in $R$ satisfying the following property:*

$$\alpha = q\beta + r, \tag{2.2}$$

*$r = 0$ or $\phi(r) < \phi(\beta)$.*

We call condition 2 the division algorithm. We chose the property $\phi(r) < \phi(\beta)$ to ensure that the division algorithm will terminate after a finite number of steps.

**Lemma 2.4.1.** *The norm function $N : \mathbb{Z}[i] \to \mathbb{Z}$ satisfies the condition $N(\alpha) \leq N(\alpha\beta)$, for any nonzero $\alpha, \beta \in \mathbb{Z}[i]$.*

*Proof.* Let $\alpha, \beta$ be nonzero Gaussian integers. We consider the norm $N$ as defined in Equation 2.1. Let $N(\alpha\beta) = N(\alpha)$. Since the norm is multiplicative we have,

$$\begin{aligned} N(\alpha)N(\beta) &= N(\alpha) \\ &= N(\alpha) \cdot 1 \\ &= N(\alpha)N(u), u \in U(\mathbb{Z}[i]). \end{aligned}$$

$\therefore N(\alpha)N(\beta) = N(\alpha)N(u)$. Applying the cancellation law we get, $N(\beta) = N(u) = 1$. Hence this condition is true when $\beta$ is a unit of $\mathbb{Z}[i]$. Now let $\beta \notin U(\mathbb{Z}[i])$ and let $\alpha = a + bi, \beta = c + di$. Then,

$$\begin{aligned} N(\alpha)N(\beta) &= N(a + bi)N(c + di) \\ &= (a^2 + b^2)(c^2 + d^2). \end{aligned}$$

Since $\alpha, \beta \neq 0$, we have

$$(a^2+b^2)(c^2+d^2) > a^2+b^2$$
$$\Rightarrow N(a+bi)N(c+di) > N(a+bi)$$
$$\therefore N(\alpha) < N(\alpha\beta).$$

□

We can use the same methodology to prove the first condition for $\mathbb{Z}$. Below is a statement of the division algorithm for $\mathbb{Z}$. The proof of the proposition can be found on Judson [14, p.26].

**Proposition 2.4.1 (Integer Division Algorithm).** *For $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist two unique integers $q$ and $r$ called the quotient and remainder respectively, such that $a = bq + r$, for $0 \leq r < |b|$.*

Combining the methodology plus the integer division algorithm above, we can see that $\mathbb{Z}$ is a Euclidean domain. We now want to prove that $\mathbb{Z}[i]$ is a Euclidean domain using Ho [13].

**Theorem 2.4.2 (Gaussian Division Algorithm).** *Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. There exists $q, r \in \mathbb{Z}[i]$ such that*

$$\alpha = \beta q + r, \tag{2.3}$$

*with $r = 0$ or $N(r) < N(\beta)$.*

*Proof.* To begin the proof we consider that $\mathbb{Z}[i] \subseteq \mathbb{C}$, hence we can represent every Gaussian integer $x + yi$ as the point $(x, y)$ in the Cartesian plane the same way we do with complex numbers. The following diagram illustrates this.

It is very important to note from the diagram that every Gaussian integer lies at the corner of a square, where each side of the square has length 1. We now want to see how we approach quotients that do not lie in $\mathbb{Z}[i]$, and hence how division operates in $\mathbb{Z}[i]$. Let $a + bi, c + di \in \mathbb{Z}[i]$. Choose $m + ni$ such that

$$\frac{a+bi}{c+di} = m + ni$$

for $m, n \in \mathbb{Q}$. Let $m+ni \notin \mathbb{Z}[i]$, then $m+ni$ does not lie at the center of a square. In fact, it lies inside a square surrounded by 4 corners $Cj$, where $j = 1; 2; 3; 4$ represents Gaussian integers at the vertex of each square with the maximum distance being $\sqrt{2}$, and the minimum distance being 1. Therefore,

$$|m + ni - Cj| < 1,\ j = 1, 2, 3, 4,$$

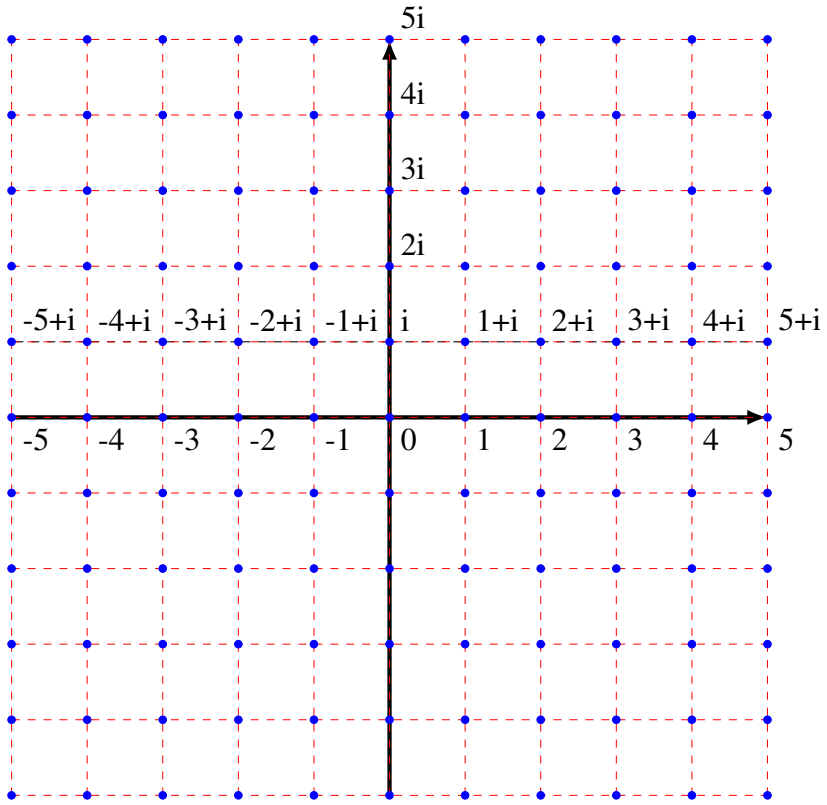



Figure 2.1: Gaussian integer square grid

as illustrated in Figure 1.1.

Since the division $\frac{a+bi}{c+di} \notin \mathbb{Z}[i]$, we want to see if we can write the division in the form $a+bi = (c+di)q+r$, where $N(r) < N(c+di)$. We pick the nearest corner $C_j$ with the coordinates $(s,t)$, where $s,t \in \mathbb{Z}$, such that,

$$|m-s| \leq \frac{1}{2} \text{ and } |n-t| \leq \frac{1}{2}.$$

Let $(a+bi) = (c+di)(m+ni)$, and $m+ni = (s+ti)+(m+ni)-(s+ti)$. Then,

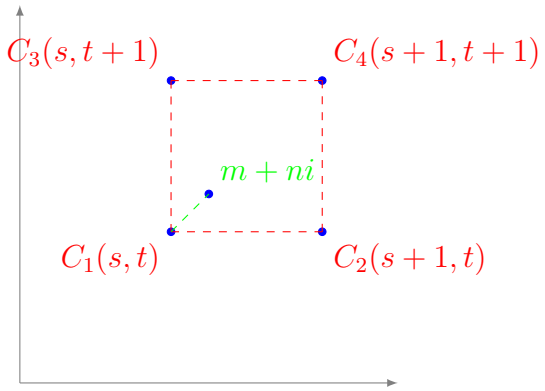



Figure 2.2: Gaussian integer square grid - 2

$$\begin{aligned} a + bi &= (c + di)(m + ni) \\ &= (c + di)[(s + ti) + (m + ni) - (s + ti)] \\ &= (c + di)(s + ti + m + ni - s - ti) \\ &= (c + di)[(s + ti) + (m - s) + (n - t)i] \\ &= (c + di)(s + ti) + (c + di)[(m - s) + (n - t)i] \end{aligned}$$

Let $r = (c + di)[(m - s) + (n - t)i]$, and $q = s + ti$. Therefore $a + bi = (c + di)q + r$. If $r = 0$, then $a + bi = (c + di)q$. If $r \neq 0$ we take the norm to get, $N(r) = N(c + di)N[(m - s) + (n - t)i]$. we will prove that $N(r) < N(c + di)$. Since $N[(m - s) + (n - t)i] = (m - s)^2 + (n - t)^2$, we have

$$N[(m - s) + (n - t)i] \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2.$$

Therefore, $N(r) \leq N(c + di)\left(\frac{1}{2}\right)$, and finally $N(r) < N(c + di)$ as desired.

□

**Corollary 2.4.2.1.** *The integral domain $R = \mathbb{Z}[i]$ is a Euclidean domain.*

*Proof.* Combining Lemma 2.4.1 and Theorem 2.4.2, we have managed to prove the existence of a $q$ and $r$ in $\mathbb{Z}[i]$, such that $\alpha = q\beta + r$, and either $r = 0$ or $N(r) < N(\beta)$. Therefore $\mathbb{Z}[i]$ is a Euclidean domain according to definition 2.4.1. □

# Chapter 3

# Divisibility and The Euclidean Algorithm

Let $R$ be a Euclidean domain as per Definition 2.4.1. Then we can find some integers $q$ and $r$ in $R$, such that $\alpha = q\beta + r$, with $r = 0$ or $\phi(r) < \phi(\beta)$. This process is called the division of $\alpha$ by $\beta$ with remainder $r$. We now consider the division of elements without a remainder.

**Definition 3.0.1.** *Let $R$ be a Euclidean domain. Choose $\beta$ in $R$. We say $\beta$ divides $\alpha$ if $\alpha = \beta k$, for some $k \in R$. We denote this as $\beta|\alpha$. We call $\beta$ a divisor of $\alpha$.*

Below are some important rules for division extracted from $\mathbb{Z}$ that we shall reference throughout the text using [11, 12].

## 3.1 Divisibility Properties and Ideals

**Proposition 3.1.1** (Properties of Divisors)**.** *Let $\alpha, \beta$ and $\gamma$ be non-zero elements of an integral domain $R$. The following hold true:*

*(i)* $\alpha|0$.

*(ii)* $0|\alpha \Rightarrow \alpha = 0$.

*(iii)* $1|\alpha$.

*(iv)* $\alpha|\alpha$.

*(v)* $\alpha\gamma|\beta\gamma \Rightarrow \alpha|\beta$, *for* $\gamma \neq 0$.

*(vi)* $\alpha|\beta$ *and* $\alpha|\gamma \Rightarrow \alpha|\beta\gamma$.

*(vii)* $\alpha|\beta$ *and* $\beta|\gamma \Rightarrow \alpha|\gamma$ .

*(viii)* $\alpha|\beta$ *and* $\alpha|\gamma \Rightarrow \alpha|(\beta+\gamma)$.

*(ix)* $\alpha|\beta$ *and* $\alpha|\gamma \Rightarrow \alpha|r\beta + s\gamma$, *for any* $r, s \in R$.

*Proof.* (i) Let $0 = k\alpha$. Since $R$ is an integral domain and $\alpha \neq 0$, $k$ can only be zero. Therefore $0 = 0\alpha$, and $\alpha|0$ for every $\alpha \in R$.
(ii) Let $0|\alpha$, then $\alpha = k0 = k(0+0 = k(0) + k(0)$ so $k0 = 0 = \alpha$.
(iii) Holds simply because $\alpha = 1$.
(iv) Let $\alpha = 1 \cdot \alpha$. Then $\alpha|\alpha$.
(v) $\alpha\gamma|\beta\gamma \Rightarrow \beta\gamma = k(\alpha\gamma) = (k\alpha)\gamma$ for some $k$ in $R$.Then $\beta\gamma = (k\alpha)\gamma$. Since $R$ is an integral domain, $\beta = k\alpha$. Therefore $\alpha|\beta$.
(vi) $\alpha|\beta$ and $\alpha|\gamma \Rightarrow \beta = k\alpha$ and $\gamma = l\alpha$ for some $k, l \in R$. By definition, $\beta = k\alpha$ and $\gamma = l\alpha$, which implies that $\beta\gamma = (kl)\alpha^2$. Let $kl = m \in R$, then $\beta\gamma = m\alpha^2$. It suffices to note that $\alpha|\beta\gamma$.
(vii) $\alpha|\beta$ and $\beta|\gamma \implies \beta = k\alpha$ and $\gamma = l\beta$ for some $k, l$ in $R$. However, $\gamma = l(k\alpha) = (lk)\alpha = m$, therefore $\alpha|\gamma$.
(viii) $\alpha|\beta$ and $\alpha|\gamma \Rightarrow \beta = k\alpha$ and $\gamma = l\alpha$, for some $k, l$ in $R$,
$(\beta+\gamma) = k\alpha+l\alpha = (k+l)\alpha$. Since $R$ is an integral domain, $(k+l) = m \in R$. Therefore $(\beta+\gamma) = m\alpha$, and $\alpha|(\beta+\gamma)$.
(ix) Let $\alpha|\beta$ and $\alpha|\gamma$. Then $\beta = k\alpha$, and $\gamma = l\alpha$ for some $k, l$ in $R$. Multiply the equation $\beta = k\alpha$ by $r$ to get $r\beta = (rk)\alpha$, and multiply the equation $\gamma = l\alpha$ by $s$ to get $s\gamma = (sl)\alpha$, for some $r, s$ in $R$. Therefore $(r\beta + s\gamma) = (rk + sl)\alpha$, which implies that $\alpha|(r\beta + s\gamma)$.

□

We will use Proposition 3.1.1 to form concepts, and prove key statements surrounding division in certain Euclidean domains in this chapter.

**Definition 3.1.1.** *A subset* $I$ *of the ring* $R$ *is called an ideal of* $R$ *if;*

- $0 \in R$.
- $\alpha, \beta \in I \Rightarrow \alpha - \beta \in I$.
- *For* $\alpha \in R$ *and* $\omega \in I$, $\alpha\omega \in I$, *and by commutativity,* $\omega\alpha \in I$ *(absorption property).*

**Proposition 3.1.2** (Operations on ideals)**.** *Let $A$ and $B$ be ideals in the ring $R$. The following is also an ideal in $R$.*

- $AB = \{\sum_{i=1}^{n} \alpha_i\beta_i : \alpha_i \in A, \beta_i \in B, i \in \mathbb{N}\}$.

We define the next property of ideals using [3].

**Definition 3.1.2.** *Let $I$ be an ideal of the ring $R$. We say the set of elements $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of the ideal $I$ generates $I$ if we can write every $\alpha$ in $I$ as a linear combination of these $\alpha_i s$ with coefficients in the ring $R$. In other words,*

$$\alpha = \sum_{i=1}^{n} \alpha_i\beta_i,$$

*with $\beta_i \in R$. Therefore we write $I = (\alpha_1, \alpha_2, \ldots \alpha_n)$.*

If $I = (0)$, $I$ is called the zero ideal, and if $I = (1)$, then $I$ is called a unit ideal.

We stated that in any ring except for the zero ring, $1 \neq 0$, hence the ideals $I = (0)$ and $I = (1)$ are different in rings which are not zero rings.

**Definition 3.1.3.** *Let $R$ be a ring. An ideal $I$ of $R$ is called a proper ideal if and only if $I \neq 0$ and $I \neq R$.*

**Remark 3.** *A proper ideal $I$ of $R$ does not contain the identity $1$ because for any $\alpha$ in $R$, if $1 \in I$, then $\alpha \cdot 1 = \alpha$ so that $I = R$. Therefore the absorption property fails.*

Let $R$ be a commutative ring, and let $I$ be an ideal of $R$. If for an element $\alpha$ of $R$ we have the equation,

$$I = (\alpha) = \{\alpha r : r \in R\},$$

then $I$ is the ideal of $R$ generated by the element $\alpha$.

**Definition 3.1.4.** *Let $R$ be an integral domain and $I \neq (0)$, an ideal in $R$. If for a single element $\alpha \in I$ we have;*

$$I = (\alpha) = \{\alpha r : r \in R\},$$

*then $I$ is called a principal ideal. An integral domain that contains only principal ideals is called a principal ideal domain (PID).*

Suppose $I = (\alpha)$ is a principal ideal in a ring $R$. If $\gamma \in I$, then $\gamma = k\alpha$, for some $k \in R$. Hence $\alpha|\gamma$. This implies that the elements of the principal ideal $(\alpha)$ are simply all the elements of $R$ that $\alpha$ divides. We use Ho [13] to prove this statement.

**Proposition 3.1.3.** *Let $R$ be an integral domain and let $\alpha$ and $\beta$ be non-zero elements of $R$. If $\beta|\alpha$ then $(\alpha) \subseteq (\beta)$.*

*Proof.* Let $\beta|\alpha$. By Definition 3.0.1, $\alpha = k_1\beta$, for some $k_1 \in R$. Let $I = (\alpha)$ be a principal ideal in $R$. If $\gamma \in I$ then $\gamma = k_2\alpha$, for some $k_2$ in $R$. By substitution we have $\gamma = k_2\alpha = k_2(k_1\beta) = (k_2k_1)\beta$, and so $\gamma \in (\beta)$. Therefore $(\alpha) \subseteq (\beta)$. □

**Lemma 3.1.1.** *If $R$ is a Euclidean domain, then $R$ is a principal ideal domain.*

*Proof.* We assume $R$ is a Euclidean domain and pick a proper ideal $I$ in $R$. Since $I$ is proper, we know that $I \neq (0); R$. Choose $\beta \neq 0$ in $I$ such that $\phi(\beta)$ is the smallest positive integer in $I$. Choose another positive integer $\alpha$ in $I$, then $\phi(\beta) < \phi(\alpha)$. Since $R$ is a Euclidean domain, we know that if we divide $\alpha$ by $\beta$, we can find integers $q$ and $r$ in $R$ such that,

$$\alpha = \beta q + r, \text{ with } r = 0 \text{ or } \phi(r) < \phi(\beta).$$

By the definition of an ideal, $\beta q \in I$ therefore $\alpha - \beta q = r \in I$. Since $\phi(\beta)$ has the smallest value by assumption, it is impossible to have $\phi(r) < \phi(\beta)$. Hence we can only have $r = 0$, and $\alpha = \beta q$. Therefore for all $k \in I$, $k = \beta q$, and $I = (\beta)$. Then $R$ is a Principal ideal domain. □

**Corollary 3.1.3.1.** *$\mathbb{Z}$, $\mathbb{Z}[i]$ are Euclidean domains.*

*Proof.* The proofs are constructed exactly like the proof for Lemma 3.0.1. □

We then discuss the concept of common divisors in the Euclidean domain $\mathbb{Z}$ using Rosen [21]. Choose elements $16$ and $24$ in $\mathbb{Z}$. From observation, the ordinary integers that divide both these numbers are,

2,4,8.

Since $2$ and $4$ are of less absolute value, we call them common divisors of $16$ and $24$. The ordinary integer 8 is then called greatest common divisor of $16$ and $24$, since it is the largest when measuring in absolute terms. In general, the next statement is true for every Euclidean domain.

**Definition 3.1.5.** *Let $R$ be a Euclidean domain, and let $\alpha$ and $\beta$ be nonzero elements of $R$. We say $\delta$ is a greatest common divisor of $\alpha$ and $\beta$ if $\delta|\alpha$ and $\delta|\beta$, and if there exists any $\delta_1$ such that $\delta_1|\alpha$ and $\delta_1|\beta$, then $\delta_1|\delta$. We denote this as $\delta = gcd(\alpha, \beta)$.*

**Theorem 3.1.4.** *Let $R$ be a principal ideal domain, and choose two non-zero elements $\alpha$ and $\beta$ in $R$. There exists an element $\delta$ in $R$ called the greatest common divisor of $\alpha$ and $\beta$, such that $(\alpha, \beta) = (\delta)$.*

*Proof.* Let $I$ be an ideal of $R$ generated by $\alpha$ and $\beta$. We denote this ideal by $I = (\alpha, \beta)$. However $R$ is a principal ideal domain, hence $R$ only contains ideals that are generated by single elements. In this case let $I = (\delta)$. We know $(\alpha) \subseteq (\alpha, \beta) = (\delta)$, hence by Proposition 3.1.3, we have $\delta|\alpha$, and $(\beta) \subseteq (\alpha, \beta) = (\delta)$,which implies that $\delta|\beta$. Lastly, to show that $\delta$ is indeed the greatest common divisor of $\alpha$ and $\beta$, we have to show that any other common divisor of $\alpha$ and $\beta$ also divides $\delta$. Let $\delta'$ be a common divisor of $\alpha$ and $\beta$. We express $\alpha$ and $\beta$ as,

$$\alpha = \delta'\alpha',$$
$$\beta = \delta'\beta'.$$

Since $\delta \in (\alpha, \beta)$, we can write $\delta$ as $\delta = \alpha r + \beta s$, for some $r, s \in R$. By substitution $\delta = (\delta'\alpha')r + (\delta'\beta')s = \delta'(\alpha' r + \beta' s)$, which implies that $\delta'|\delta$. Therefore $\delta$ is the greatest common divisor of $\alpha$ and $\beta$. □

**Theorem 3.1.5.** *Let $R$ be a Euclidean domain with nonzero $a, b$ in $R$, and let $\delta = gcd(\alpha, \beta)$. Then $\delta = gcd(\alpha, \beta)$ is unique up to order of units.*

*Proof.* Let $\delta_1$ and $\delta_2$ be greatest common divisors of $\alpha$ and $\beta$. Then $\delta_1 = gcd(\alpha, \beta)$, and by definition $\delta_1|\alpha$ and $\delta_1|\beta$. Since $\delta_2$ is also a greatest common divisor of $\alpha$ and $\beta$, we know $\delta_2|\alpha$ and $\delta_2|\beta$. Then

$$\delta_2|\delta_1 \text{ and } \delta_2|\delta_1.$$

This implies that $\delta_1 = r\delta_2$ and $\delta_2 = s\delta_1$. By substitution $\delta_1 = r(s\delta_1) = (rs)\delta_1$. Therefore $1 \cdot \delta_1 = (rs)\delta_1$, and by the right cancellation law we have $1 = rs$. By Definition 2.2.2, the elements $r$ and $s$ are units. Therefore by Definition 2.2.3, $\delta_1$ and $\delta_2$ are associates.

□

How does one find the greatest common divisor of two numbers? The Euclidean algorithm is a method that was developed to make the process of finding greatest common divisors very efficient.

**Remark 4.** *Let $R$ be a Euclidean Domain. The following method is called the Euclidean algorithm, and it terminates after a finite number of steps. In the Euclidean domain $R$, to find the greatest common divisor of two integers $\alpha$ and $\beta$, we follow these steps,*

$$\begin{aligned} \alpha &= q_1\beta + r_1 \qquad \phi(r_1) < \phi(\beta) \\ \beta &= q_2 r_1 + r_2 \qquad \phi(r_2) < \phi(r_1) \end{aligned}$$

*and*

$$\begin{aligned} r_1 &= r_2 q_3 + r_3 \qquad \phi(r_3) < \phi(r_2) \\ r_2 &= r_3 q_4 + r_4 \qquad \phi(r_4) < \phi(r_3) \\ &\vdots \\ r_{k-1} &= r_k q_{k+1} + r_{k+1} \quad \phi(r_{k+1}) < \phi(r_k) \\ r_k &= r_{k+1} q_{k+2}. \end{aligned}$$

*We call $r_{k+1}$ the greatest common divisor of $\alpha$ and $\beta$, as it divides both of them, and every other remainder in the algorithm which can be seen on Judson [14, p.29].*

With this information we want to introduce prime elements to understand the concept of a greatest common divisor even further. For $\mathbb{Z}$ a prime number $p$ is an element that is divisible by $1$ and $p$ only. For other domains, we will use the following property.

**Definition 3.1.6.** *An element $p$ of $R$ is called a prime element if $p \notin U(R)$, and if $p|\alpha\beta$, then either $p|\alpha$, or $p|\beta$.*

**Definition 3.1.7.** *Let $\alpha, \beta \in R$. If $gcd(\alpha, \beta) = 1$, then $\alpha$ and $\beta$ are said to be relatively prime in $R$.*

In this case, the term relatively prime just alludes to the fact that the only common divisors between the two elements are the units of $R$. In $\mathbb{Z}$ said elements are $\pm 1$, the units of $\mathbb{Z}$. We will then state Euclid's algorithm, and for the proof we will use the Well-Ordering Principle which uses the concept of a subset. A set $A$ is a subset of $B$ if every element of the set $A$ is in the set $B$.

**Definition 3.1.8** (The Well-Ordering Principle)**.** *Every non-empty subset of natural numbers is well-ordered.*

**Theorem 3.1.6** (Euclid's Algorithm)**.**

- *Let $\delta = gcd(\alpha, \beta)$ for nonzero $\alpha, \beta \in \mathbb{Z}$. If there exists some $\delta_1$ in $\mathbb{Z}$ such that $\delta_1|\alpha$ and $\delta_1|\beta$, then $\delta_1|\delta$.*

- *There exists* $r, s \in \mathbb{Z}$ *such that* $\delta = gcd(\alpha, \beta) = r\alpha + s\beta$.

*Proof.* We proved the first item in Theorem 3.1.5. We prove the second item. Let $S = \{\alpha u + \beta v | \alpha u + \beta v > 0\}$. Then $S$ is a non-empty set. By the Well-Ordering Principle the set $S$ contains an element smaller than all the other elements in the set. Let $\delta = \alpha r + \beta s$ be the smallest element, and let $\delta = gcd(\alpha, \beta)$. We write $\alpha = \delta q + r$, where $0 \leq r < d$. Then if $r > 0$ we have,

$$\begin{aligned} r &= \alpha - \delta q \\ &= \alpha - (\alpha r + \beta s)q \\ &= \alpha - \alpha r q - \beta s q \\ &= \alpha(1 - rq) + \beta(sq). \end{aligned}$$

Therefore $r$ is in the set $S$. However this contradicts the fact that $\delta$ is the smallest element of $S$. Therefore $r = 0$ and $\delta | \alpha$. We can use the same argument to prove that $\delta | \beta$. □

**Corollary 3.1.6.1.** *Let* $\alpha$ *and* $\beta$ *be ordinary integers. If* $\delta = gcd(\alpha, \beta) = 1$*, then there exist* $r, s \in \mathbb{Z}$*, such that*

$$r\alpha + s\beta = 1.$$

We use Judson [14] to introduce a property of Euclid for integers.

**Proposition 3.1.7** (Euclid's Lemma)**.** *Let* $\alpha$ *and* $\beta$ *be integers, and* $p$ *be prime in* $\mathbb{Z}$*.*

*If* $p | \alpha\beta$*, then either* $p | \alpha$ *or* $p | \beta$*.*

*Proof.* Let $p | \alpha\beta$, but $p \nmid \alpha$. We have to show that $p | \beta$. Since $p$ is prime, $gcd(\alpha, p) = 1$. By the preceding Corollary, there exists $r, s \in \mathbb{Z}$ such that,

$$\alpha r + ps = 1.$$

Then $\beta = \beta \cdot 1 = \beta(\alpha r + ps) = (\alpha\beta)r + p(\beta s)$. We know $p | p$ and $p | \alpha\beta$, therefore $p | \beta = (\alpha\beta)r + p(\beta s)$. □

## 3.2 Gaussian Integer Division

Now that we have seen how division operates in $\mathbb{Z}$, we want to see if we can carry the same theory from $\mathbb{Z}$ and apply it to Gaussian integers. Since $\mathbb{Z}[i]$ is an integral domain, we choose two non-zero Gaussian integers $\alpha$, and $\beta$. We say $\alpha|\beta$ if

$$\beta = \eta\alpha, \text{ for some } \eta \in \mathbb{Z}[i].$$

We carry out division in $\mathbb{Z}[i]$ with the same rules that govern division in $\mathbb{C}$. In other words,

$$\begin{aligned}\frac{a+bi}{c+di} &= \frac{a+bi}{c+di}\cdot\frac{c-di}{c-di}\\ &= \frac{(a+bi)(c-di)}{(c-di)(c-di)}\\ &= \frac{(ac+bd)+(bc-ad)i}{c^2+d^2}\\ &= \frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i \in \mathbb{Z}[i].\end{aligned}$$

**Example 2.** *We want to check if* $1+2i|1+7i$*, and* $1+5i|3+3i$.

$$\begin{aligned}\frac{1+7i}{1+2i} &= \frac{(1+7i)(1-2i)}{(1+2i)(1-2i)}\\ &= \frac{1-2i+5i+14}{(1)^2-(2i)^2}\\ &= \frac{15+5i}{5} = 3+i \in \mathbb{Z}[i].\end{aligned}$$

$\therefore 1+2i|1+7i.$

$$\begin{aligned}\frac{3+3i}{1+5i} &= \frac{3+3i}{1+5i}\cdot\frac{1-5i}{1-5i}\\ &= \frac{(3+3i)(1-5i)}{(1+5i)(1-5i)}\\ &= \frac{3-15i+3i+15}{(1)^2-(5i)^2}\\ &= \frac{18-12i}{26}\\ &= \frac{18}{26}-\frac{12i}{26} = \frac{9}{13}-\frac{6}{13}i.\end{aligned}$$

$\therefore 1+5i \nmid 3+3i.$

**Proposition 3.2.1.** *Let $\alpha$ and $\beta$ be arbitrary Gaussian integers. If $\alpha|\beta$ in $\mathbb{Z}[i]$, then $N(\alpha)|N(\beta)$ in $\mathbb{Z}$.*

*Proof.* Let $\alpha|\beta$, then by definition $\beta = \eta\alpha$, for some $\eta \in \mathbb{Z}[i]$.

$$N(\beta) = N(\eta\alpha) = N(\eta)N(\alpha).$$

$\therefore$ Since $N(\eta) \in \mathbb{Z}$, we can conclude that $N(\alpha)|N(\beta)$. □

We look at some examples. We first have $1+2i|1+7i$. Applying the norm we get

$$N(1+2i) = 5|N(1+7i) = 50$$

showing that the proposition is true.

We now want to check if the converse of this proposition is true. In other words, if $N(\alpha)|N(\beta)$ in $\mathbb{Z}$, does this mean $\alpha|\beta$ in $\mathbb{Z}[i]$? Let us look at some interesting examples. Let $\alpha = 4+i$ with $N(4+i) = 17$ and $\beta = 3+5i$ with $N(3+5i) = 34$. Then $N(4+i) = 17|34 = N(3+5i)$ in $\mathbb{Z}$.

$$\begin{aligned}\frac{3+5i}{4+5i} &= \frac{3+5i}{4+i}\cdot\frac{4-i}{4-i}\\ &= \frac{(3+5i)(4-i)}{(4+i)(4-i)}\\ &= \frac{12-3i+20i-5i^2}{(4)^2-(i)^2}\\ &= \frac{17+17i}{17}\\ &= \frac{17}{17}+\frac{17i}{17}\\ &= 1+i.\end{aligned}$$

$\therefore 4+i|3+5i.$

Let $\alpha = 4-i$ with $N(4-i) = 17$ and $\beta = 3+5i$ with $N(3+5i) = 34$. Then $N(4-i) = 17|34 = N(3+5i)$ in $\mathbb{Z}$.

$$\begin{aligned}\frac{3+5i}{4-i} &= \frac{3+5i}{4-i}\cdot\frac{4+i}{4+i}\\ &= \frac{(3+5i)(4+i)}{(4-i)(4+i)}\\ &= \frac{12+3i+20i-5}{(4)^2-(i)^2}\\ &= \frac{7+23i}{17}\\ &= \frac{7}{17}+\frac{23}{17}i.\end{aligned}$$

$\therefore 4-i \nmid 3+5i.$

Which proves that the converse is not true.

**Example 3.** *We want to continue with the last example where we encountered division with remainder. As a result, we will use the Gaussian Division Algorithm to find the quotient $q$ and remainder $r$, satisfying the norm condition*

$$N(r) < N(1+5i).$$

*Let* $m = \frac{9}{13}$, *and* $n = -\frac{6}{13}$. *We begin by finding* $s, t \in \mathbb{Z}$ *such that,*

$$|m - s| = \left|\frac{9}{13} - s\right| \leq \frac{1}{2}$$
$$|n - t| = \left|-\frac{6}{13} - t\right| \leq \frac{1}{2}.$$

*Choose integers* $s = 1$ *and* $t = 0$ *since*

$$|m - s| = \left|\frac{9}{13} - 1\right| < \frac{1}{2}$$
$$|n - t| = \left|-\frac{6}{13} - 0\right| < \frac{1}{2}.$$

*Hence* $q = s + ti = 1 + 0i$ *is our quotient, and to finish the division we let,*

$$r = \alpha - q\beta = (3 + 3i) - (1 + 0i)(1 + 5i) = 2 - 2i.$$

*We now check if the norm condition is satisfied.*

$$N(2 - 2i) = (2)^2 + (-2)^2 = 8 < N(1 + 5i) = (1)^2 + (5)^2 = 26.$$

$\therefore 3 + 3i = (1 + 5i)(1 + 0i) + 2 - 2i.$

As in $\mathbb{Z}$, we can repeatedly apply the Gaussian division algorithm to $\frac{\alpha}{\beta}$.

**Theorem 3.2.2** (Calcut [6])**.** *The Euclidean algorithm for Gaussian integers.*

*Proof.* We pick any two nonzero Gaussian integers $\alpha$ and $\beta$. We want to compute $\frac{\alpha}{\beta}$ using the Gaussian division algorithm. The first line we get is,

$$\alpha = q_1\beta + r_1 \quad where \quad 0 < N(r_1) < N(\beta).$$

If $r_1 = 0$, we stop. Otherwise we continue the procedure until we reach an iteration where $r = 0$.

For our next step, we divide $\beta$ by $r_1$, and so on until we reach that last iteration. Therefore,

$$\begin{gathered}\beta = q_2 r_1 + r_2 \quad where \quad 0 < N(r_2) < N(r_1) \\ r_1 = q_3 r_2 + r_3 \quad where \quad 0 < N(r_3) < N(r_2) \\ \vdots \\ r_{l-1} = q_{l+1} r_l + r_{l+1} \quad where \quad 0 < N(r_{l+1}) < N(r_1) \\ r_l = q_{l+2} r_{l+1} + 0.\end{gathered}$$

Notice that $N(\beta) > N(r_1) > N(r_2) > N(r_3) > \ldots > N(r_{l+1})$. This will be the basis for factorization in the next chapter. The Euclidean algorithm for $\mathbb{Z}[i]$ terminates because one cannot have an infinite, decreasing sequence of natural numbers since they are well-ordered. Just like in $\mathbb{Z}$, the last remainder $r_{l+1}$ is the greatest common divisor of $\alpha$ and $\beta$. To show this we can work from the last equation of the algorithm going upwards.

□

We also have the concept of the greatest common divisor in $\mathbb{Z}[i]$ as a result of $\mathbb{Z}[i]$ being a Euclidean domain.

**Definition 3.2.1.** *Let $\alpha$ and $\beta$ be nonzero Gaussian integers. We say $\delta$ is a greatest common divisor of $\alpha$ and $\beta$ if $\delta|\alpha$ and $\delta|\beta$, and if there exists any $\delta_1$ such that $\delta_1|\alpha$ and $\delta_1|\beta$, then $\delta_1|\delta$. We denote this as $\delta = gcd(\alpha, \beta)$.*

**Theorem 3.2.3** (Euclid's Algorithm For Gaussian Integers)**.**

- *Let $\delta = gcd(\alpha, \beta)$ for nonzero $\alpha, \beta \in \mathbb{Z}[i]$. If there exists some $\delta_1$ in $\mathbb{Z}[i]$ such that $\delta_1|\alpha$ and $\delta_1|\beta$, then $\delta_1|\delta$.*
- *There exists $r, s \in \mathbb{Z}[i]$ such that $\delta = gcd(\alpha, \beta) = r\alpha + s\beta$.*

*Proof.* The proof is similar to the proof for $\mathbb{Z}$. □

**Definition 3.2.2.** *Let $\alpha$ and $\beta$ be Gaussian integers. If*

$$gcd(\alpha, \beta) = 1,$$

*then $\alpha$ and $\beta$ are relatively prime in $\mathbb{Z}[i]$.*

Finding the greatest common divisor of two integers in $\mathbb{Z}[i]$ becomes slightly more complex because we are now working in $2D$ as shown in the proof of the Gaussian integer division algorithm. We use an example to illustrate this complexity we speak of.

**Example 4.** *We want to find $gcd(1 + i, -1 + 6i)$ using the Euclidean Algorithm for $\mathbb{Z}[i]$. We first incorporate the division algorithm for $\mathbb{Z}[i]$.*

$$\frac{-1+6i}{1+i} = \frac{5}{2} + \frac{7}{2}i = m + ni.$$

*Let* $m = \frac{5}{2}$ *and* $n = \frac{7}{2}$. *We want to find integers* $s$ *and* $t$ *such that,*

$$|m-s| = \left|\frac{5}{2} - s\right| \leq \frac{1}{2}$$
$$|n-t| = \left|\frac{7}{2} - t\right| \leq \frac{1}{2}.$$

*To assist us we plot the position of the quotient* $\frac{5}{2} + \frac{7}{2}i$ *in the complex plane.*

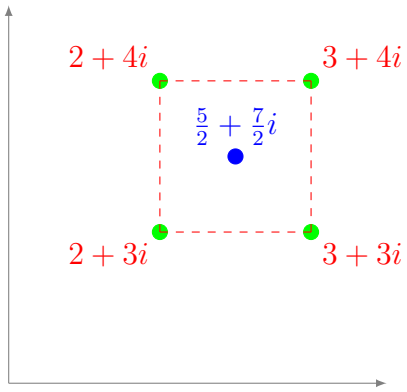



Figure 3.1: Gaussian integer square grid - 3

*If we look at the illustration it shows us that we have 4 possible choices for the quotient, viz,* $2+3i, 2+4i, 3+3i, 3+4i$. *We check if they satisfy the necessary conditions.*

*We first check if the values for* $s$ *work. We have* $s = 2, 3$.

$$|m-s|\, t = \left|\frac{5}{2} - 2\right| = \frac{1}{2}$$
$$|m-s| = \left|\frac{5}{2} - 3\right| = \left|-\frac{1}{2}\right| = \frac{1}{2}.$$

$\therefore$ *We will choose either* $s = 2$ *or* $s = 3$ *for our quotient. Now we verify the values for* $t = 3, 4$.

$$|n-t| = \left|\frac{7}{2} - 3\right| = \frac{1}{2}$$
$$|n-t| = \left|\frac{7}{2} - 4\right| = \left|-\frac{1}{2}\right| = \frac{1}{2}.$$

*Let* $N\left(\dfrac{-1+6i}{1+i}\right) = N\left(\dfrac{5}{2}+\dfrac{7}{2}i\right)$

$$N\left[\left(\frac{5}{2}+\frac{7}{2}i\right) - (2+3i)\right] = N\left(\frac{1}{2}+\frac{1}{2}i\right) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$
$$N\left[\left(\frac{5}{2}+\frac{7}{2}i\right) - (2+4i)\right] = N\left(\frac{1}{2}+-\frac{1}{2}i\right) = \left(\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$
$$N\left[\left(\frac{5}{2}+\frac{7}{2}i\right) - (3+3i)\right] = N\left(-\frac{1}{2}+\frac{1}{2}i\right) = \left(-\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$
$$N\left[\left(\frac{5}{2}+\frac{7}{2}i\right) - (3+4i)\right] = N\left(-\frac{1}{2}+-\frac{1}{2}i\right) = \left(-\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right)^2 = \frac{1}{2} < 1.$$

*Hence all four quotients work. We will then find* $r$ *using the formula,*

$$r = \alpha - [(\beta)(q)] = (-1+6i) - [(1+i)(s+ti)],$$

*which in turn gives us the following solutions for each quotient.*

$$-1+6i = (1+i)(2+3i) + i$$
$$-1+6i = (1+i)(2+4i) + 1$$
$$-1+6i = (1+i)(3+3i) - 1$$
$$-1+6i = (1+i)(3+4i) - i.$$

$\therefore$ *Since* $gcd(-1+6i, 1+i) = \{1, i, -1, -i\} = U(\mathbb{Z}[i])$*, we can conclude that* $-1+6i$ *and* $1+i$ *are relatively prime* $\mathbb{Z}[i]$.

What this example and the Euclidean algorithm for $\mathbb{Z}[i]$ has shown us is that, in $\mathbb{Z}[i]$, we can have more than a single choice for our quotient after division since $\dfrac{\alpha}{\beta}$ lies inside a square with 4 possible corners to choose from. When the quotient $m+ni$ lies at the center of the square, we will have exactly four choices. This implies that the quotient $q$ and the remainder $r$ are not unique, unlike in the ring $\mathbb{Z}$ where both are guaranteed to be unique.

**Remark 5.** *Let $\alpha$ and $\beta$ be non-zero Gaussian integers. If $\beta|\alpha$, then $\alpha = \eta\beta + 0$, for some $\eta \in \mathbb{Z}[i]$. Hence $gcd(\alpha, \beta) = \beta$. If $\beta \nmid \alpha$, then $\alpha = \beta q + r$ where $N(r) < N(\alpha)$.*

The following property follows from the concept of divisibility in $\mathbb{Z}[i]$.

**Proposition 3.2.4.** *Let $a + bi$ be a Gaussian integer and $\gamma \in \mathbb{Z}$. Then $\gamma|a + bi$ if and only if $\gamma|a$ and $\gamma|b$.*

*Proof.* Note that,

$$\gamma|a + bi \Leftrightarrow a + bi = (r + si)(\gamma) \Leftrightarrow a = r(\gamma), b = s(\gamma).$$

Hence $\gamma|a$ and $\gamma|b$, for some $r + si \in \mathbb{Z}[i]$. □

Therefore, divisibility in the ring $\mathbb{Z}$ is just divisibility in $\mathbb{Z}[i]$, where $b = 0$.

# Chapter 4

# Factorization

## 4.1 Factorization in $\mathbb{Z}$

As Chapter 3 progressed, we learnt of a set of integers called prime integers in $\mathbb{Z}$, and as we mentioned in the introduction, The Fundamental Theorem of Arithmetic states that every non-zero ordinary integer can be broken down into a product of primes by a process called factorization, and that this particular factorization is unique up to units. In this chapter, we want to gain further insight on the significance of prime elements in an integral domain, by studying their existence and uniqueness, and how these two concepts relate to our understanding of factorization in $\mathbb{Z}[i]$, and other integral domains, using [14, 25]. We begin by introducing the following definitions.

**Definition 4.1.1.** *Let $R$ be an integral domain. We define an irreducible element of $R$ to be a nonzero, non-unit element $\gamma \in R$ such that if $\gamma = \alpha_1\alpha_2$, then either $\alpha_1$ or $\alpha_2$ is a unit of $R$.*

**Definition 4.1.2.** *Let $R$ be an integral domain. We define a reducible element of $R$ to be a nonzero, non-unit element that is not irreducible.*

We want to prove that indeed every non-zero element of $\mathbb{Z}$ can be factored into a product of primes using Judson [14]. Note that we will call integers ordinary integers sometimes to differentiate them from Gaussian integers.

**Theorem 4.1.1** (Existence of Factorization In $\mathbb{Z}$)**.** *Let $\gamma \neq 0$ be an arbitrary ordinary integer. Then $\gamma$ can be written in the form;*

$$\gamma = u\alpha_1 \cdots \alpha_k, \text{ for } k \in \mathbb{N},$$

*where $u = \pm 1$, and $\alpha_i$ represents positive ordinary integer primes.*

*Proof.* Suppose we can find $\gamma$ in $\mathbb{Z}$, such that $\gamma$ cannot be factored into a product of integer primes. Define $S$ to be the set that contains all $\gamma$ in $\mathbb{Z}$, such that $\gamma$ cannot be factored into a product of primes. Then by the Well-Ordering Principle the set $S$ contains an element with the least absolute value than all the other elements in the set. Let $\beta$ be such an element. We have two cases for $\beta$.

Case 1: $\beta = \beta \cdot 1$, this is always true since $\beta = \beta \cdot 1$ is the only factorization of $\beta$ up to units.

Case 2: $\beta = \beta_1\beta_2$.

In case 1, $\beta > 0 \notin S$, since $\beta$ is prime.

In case 2, $1 < \beta_1 < \beta$, and $1 < \beta_2 < \beta$, but since $\beta$ is the smallest element of $S$, we have that $\beta_1, \beta_2 \notin S$. Hence we can write $\beta_1$ and $\beta_2$ as a product of other ordinary integer primes:

$$\beta_1 = p_1p_2 \dots p_j$$
$$\beta_2 = q_1q_2 \dots p_k.$$

Substituting the factorizations of $\beta_1$ and $\beta_2$ into case 2, we have,

$$\beta = \beta_1\beta_2 = p_1p_2 \dots p_jq_1q_2 \dots p_k.$$

A contradiction since we stated that $\beta \in S$, and cannot be factored into a product of primes. □

Having seen that prime factorization is possible in $\mathbb{Z}$, we want to learn about the concept of uniqueness of factorization, which is the second element of The Fundamental Theorem of Arithmetic using Judson [14]. The question this concept poses is "is it possible to have more than one factorization in an integral domain, and if it is, what are the consequences?".

**Definition 4.1.3.** *Let $R$ be an integral domain, R is called a unique factorization domain (UFD), if every non-zero element $\gamma \in R$ can be written uniquely as $\gamma = u\alpha_1 \cdots \alpha_k$, for some $k \in \mathbb{N}$, where $u \in U(R)$, and $\alpha_i$ are irreducible elements of R. Furthermore, this factorization into irreducibles is unique except for reordering, and multiplication by units.*

**Theorem 4.1.2** ($\mathbb{Z}$ is a Unique Factorization Domain)**.** *Every non-zero integer $\gamma > 1$ can be factored into $\gamma = u\alpha_1 \cdots \alpha_k$, for some $k \in \mathbb{N}$, where $u = \pm 1$, and $\alpha_i$ are positive prime ordinary integers. Furthermore, this prime factorization is unique upto reordering, and multiplication by units.*

*Proof.* Let $\gamma$ be an ordinary integer and let the following be two factorizations of $\gamma$ into the prime elements of $\mathbb{Z}$.

$$(\pm 1)\alpha_1 \cdots \alpha_m = \gamma = (\pm 1)\beta_1 \cdots \beta_n,$$

with $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$ and $\beta_1 \leq \beta_2 \leq \ldots \leq \beta_m$.

We want to prove that these two factorizations are the same. We use induction on $\gamma$.

Let $\gamma = 1$, $\gamma$ is a unit and we do not consider this case.

Let $\gamma = 2$, then $\gamma$ is prime, and we have the desired result.

We then assume that the results hold for all ordinary integers $\rho$ such that $1 \leq \rho < \gamma$. By Euclid's Lemma, $\alpha_1 | \beta_i$ for some $i = 1, \ldots, n$, and $\beta_1 | \alpha_j$ for some $j = 1, \ldots, m$. Since all $\alpha_i$'s and $\beta_i$'s are prime, we have $\alpha_1 = \beta_i$ and $\beta_1 = \alpha_j$. Therefore $\alpha_1 = \beta_1$ since $\alpha_1 \leq \alpha_j = \beta_1 \leq \beta_i = \alpha_1$. Using induction,

$$\gamma' = \alpha_2 \cdots \alpha_m = \beta_2 \cdots \beta_n,$$

can be factored uniquely. Therefore $m = n$ and $\alpha_i = \beta_i$ for $i = 1, \ldots, m$.

□

By definition, every element in a UFD must be written as a product of irreducible elements from the same integral domain. In the integral domain $\mathbb{Z}$, irreducible and prime elements are one and the same, but this might not be the case for other integral domain. We reference $\mathbb{Z}$ to explore the relationship between prime and irreducible elements in an arbitrary integral domain further.

**Theorem 4.1.3.** *Let $R$ be an integral domain, and let $\gamma \in R$. We claim that if $\gamma$ is prime in $R$, then $\gamma$ is also irreducible in $R$.*

*Proof.* Choose $\gamma \neq 0$ in $R$. Assume $\gamma$ is prime but not irreducible. Then by definition of reducible elements, $\gamma = \alpha_1 \alpha_2$, where neither $\alpha_1$ nor $\alpha_2$ is a unit in R.

Generalizing the definition of prime elements in $\mathbb{Z}$ to arbitrary integral domains, we get that

$$\text{if } \gamma | \alpha_1 \alpha_2, \text{ then } \gamma | \alpha_1 \text{ or } \gamma | \alpha_2.$$

Suppose $\gamma | \alpha_1$, then $\alpha_1 = (\gamma)\beta$, for some $\beta$ in $R$. Substituting back we have,

$$\gamma = (\gamma\beta)\alpha_2 = \gamma(\beta\alpha_2).$$

Since $R$ is an integral domain, we use the cancellation law and are left with the equation $1 = (\beta)\alpha_2$.

Hence $\alpha_2|1$, and consequently $\alpha_2$ is a unit, but we said none of $\alpha_1$ or $\alpha_2$ is a unit, hence we obtain a contradiction.

$\therefore$ If $\gamma$ is prime in $R$ then $\gamma$ is irreducible in $R$. □

**Remark 6.** *In a principal ideal domain $R$, every irreducible element of $R$ is prime in $R$. Let $p, \alpha, \beta$ in $R$, where $p|\alpha\beta$. Let $\delta = gcd(p, \alpha)$. If $\delta \in U(R)$, then by 3.1.7, $p$ and $\alpha$ are relatively prime. Then Ho [13, p.30] proves that if $p|\alpha\beta$, and $p, \alpha$ are relatively prime, then $p|\beta$. If $\delta$ is not a unit then we can express $p$ as $p = \delta u$. However since $p$ is irreducible, $u \in U(R)$. By Definition 2.2.2, $p$ and $\delta$ are units, which implies that $p|\alpha$ as desired. We will show an example of what happens if this is not the case in an integral domain.*

From the statements above we can conclude that irreducible and prime elements are one and the same if only if the domain in which they exist is a UFD. In any other domain that does not satisfy this property, we cannot conclude this result.

We focus the next subsection on understanding factorization in $\mathbb{Z}[i]$.

## 4.2 Gaussian Integer Factorization

For this section we discuss Factorization in $\mathbb{Z}[i]$ using [1, 2].

**Theorem 4.2.1** (The Existence of Gaussian integer Factorization)**.** *Every non-zero, non-unit Gaussian integer can be written as a product of Gaussian irreducibles in the form*

$$\gamma = u\alpha_1 \cdots \alpha_k, \text{ for } k \in \mathbb{N},$$

*where $u \in \{1, i, -1, -i\}$, and $\alpha_i$ are irreducibles in $\mathbb{Z}[i]$.*

*Proof.* We pick any arbitrary non-zero, non-unit Gaussian integer and prove that it can be written as a product of irreducible elements of $\mathbb{Z}[i]$, by induction on $N(\gamma)$. If $\gamma$ is a Gaussian irreducible, we are done. Suppose it is otherwise, then $\gamma = (a + bi)(c + di)$, where $a + bi$, and $c + di$ are non-units. Therefore,

$$\begin{aligned} N(\gamma) &= N[(a + bi)(c + di)] \\ &= N(a + bi)N(c + di). \end{aligned}$$

Since $a + bi$, and $c + di$ are non-units, $N(a + bi), N(c + di) \neq 1$, therefore

$$N(a+bi), N(c+di) < N(\gamma).$$

It follows that $a+bi$ and $c+di$ are products of Gaussian irreducibles. Hence $\gamma = (a+bi)(c+di)$ is a factorization of $\gamma$ into a product of Gaussian irreducibles. This is true because if we continue the process it will terminate, since when $\gamma$ is non-zero, the norm is a natural number. □

**Lemma 4.2.1** (Euclid's Lemma for Gaussian integers)**.** *Let $\gamma, \alpha, \beta$ be a Gaussian integers. If $\gamma$ is prime in $\mathbb{Z}[i]$, and $\gamma|\alpha\beta$, then either $\gamma|\alpha$ or $\gamma|\beta$.*

*Proof.* The proof is similar to the proof of Euclid's Lemma for $\mathbb{Z}$. We just replace the ordinary integers with the Gaussian integers. □

Note that we use the definition of primes in $\mathbb{Z}[i]$ because $\mathbb{Z}[i]$ is a Euclidean domain. We will study the different types of Gaussian primes in detail in Chapter 6.

**Theorem 4.2.2** (Uniqueness of Gaussian Integer Factorization)**.** *Every non-zero, non-unit Gaussian integer $\gamma$ can be written as a product of Gaussian irreducibles in the form $\gamma = u\alpha_1 \cdots \alpha_k$, for $k \in \mathbb{N}$, where $u \in \{1, i, -1, -i\}$, and $\alpha_i$ are irreducibles in $\mathbb{Z}[i]$. Furthermore, when this factorization exists, it is unique up to order of units and associates.*

*Proof.* Let $\gamma = u\alpha_1 \cdots \alpha_k$, and $\gamma = u\beta_1 \cdots \beta_l$ be two factorizations of the Gaussian integer $\gamma$ into the Gaussian irreducibles $\alpha_m$ and $\beta_n$. Let us assume that these two factorizations are not equal. Then cancelling all the common factors in the factorizations, assume we have,

$$\alpha_1 \cdots \alpha_k = \gamma = \beta_1 \cdots \beta_l,$$

where $\alpha_m \neq u\beta_n$, for any $m, n \in \mathbb{N}$, and $u \in U(\mathbb{Z}(i))$. Then $\alpha_1 | \beta_1 \cdots \beta_l$. Since $\alpha_1$ is irreducible, $\alpha_1$ is also prime, therefore by Euclid's Lemma for Gaussian integers, either $\alpha_1|\beta_1$ or $\alpha_1|(\beta_2 \cdots \beta_l)$. Since $\alpha_m \neq u\beta_n$, $\alpha_1 \nmid \beta_1$. Therefore, $\alpha_1|(\beta_2 \cdots \beta_l)$. We repeat this process until we get to $\alpha_1|\beta_l$, which is a contradiction.

□

If we combine Theorem 4.2.1 and Theorem 4.2.2, we get The Fundamental Theorem of arithmetic for Gaussian Integers. Notice that since $\mathbb{Z}[i]$ is a unique factorization domain, every irreducible is prime. This means for the rest of this chapter we will not have to worry about the characterization of Gaussian primes. We will discuss Gaussian primes in Chapter 5.

**Corollary 4.2.2.1.** *Suppose $\alpha$ is a Gaussian irreducible. Then the following is true.*

- *$u\alpha$, for all $u \in U(\mathbb{Z}[i])$, is irreducible.*
- *$\overline{\alpha}$ is a Gaussian irreducible.*
- *$\alpha$ has only 8 divisors in $\mathbb{Z}[i]$, viz, $\pm 1, \pm i, \pm\alpha, \pm i\alpha$.*

We will give the results of this Corollary in Chapter 6.

Using the given information and Butler [5], we want to formulate a general method for factorization in $\mathbb{Z}[i]$.

**Remark 7** (Gaussian Integer Factorization Algorithm)**.** *Let $\alpha$ be a nonzero non-unit Gaussian integer. We can prove that $\alpha$ is reducible using the following method. Let $\beta$ and $\gamma$ be non-unit Gaussian integer factors of $\alpha$. Then $\alpha = \beta\gamma$. Taking the norm we get $N(\alpha) = N(\beta)N(\gamma)$. Taking $\beta = a + bi$, and $\gamma = c + di$, we get $N(\alpha) = (a^2 + b^2)(c^2 + d^2)$. Since $N(\alpha)$ is an integer, we can use The Fundamental Theorem of Arithmetic to factor $N(\alpha)$ into $N(\alpha) = XY$, where $X$ and $Y$ are non-unit integers. Then $(a^2 + b^2)(c^2 + d^2) = XY$, which gives us,*

$$(a^2 + b^2) = X \text{ and } (c^2 + d^2) = Y.$$

*We then solve for these two equations to find $a, b, c, d \in \mathbb{Z}$, such that,*

$$(a + bi)(c + di) = \alpha.$$

**Corollary 4.2.2.2.** *The Gaussian integer $1 + i$ is irreducible $\mathbb{Z}[i]$.*

*Proof.* We know that the elements of $\mathbb{Z}[i]$ are of the form $a + bi$, for $a, b \in \mathbb{Z}$. So the factorization of $1+i$ takes the form, $1+i = (\pm a \pm bi)(\pm c \pm di)$, where neither $\pm a \pm bi$, nor $\pm c \pm di$ are units.

We want to check if this equation and the assumption we made is true. To do so, we assess the norm of the Gaussian integer in question.

$$\begin{aligned} N(1 + i) &= N[(\pm a \pm bi)(\pm c \pm di)] \\ 2 &= N(\pm a \pm bi)N(\pm c \pm di) \\ 2 \cdot 1 &= (a^2 + b^2)(c^2 + d^2). \end{aligned}$$

This gives us the equations $(a^2 + b^2) = 2$, and $(c^2 + d^2) = 1$, because 2 is an ordinary prime. The Gaussian integer $1+i$ is irreducible since $c+di$ is a unit. □

We want to see how this theorem applies to Gaussian reducibles.

**Example 5.** *We want to check if the Gaussian integer $1+3i$ is irreducible in $\mathbb{Z}[i]$. Suppose we can write the Gaussian integer in the form,*

$$1+3i = (\pm a \pm bi)(\pm c \pm di),$$

*where neither $a+bi$, nor $c+di$ is a unit. Then to verify if this is possible we check the norm.*

$$\begin{aligned} N(1+3i) &= N[(\pm a \pm bi)(\pm c \pm di)] \\ (1)^2 + (3)^2 &= N(\pm a \pm bi)N(\pm c \pm di) \\ 10 &= (a^2+b^2)(c^2+d^2) \\ 2 \cdot 5 &= (a^2+b^2)(c^2+d^2). \end{aligned}$$

*We let $2 = a^2+b^2$, and $5 = c^2+d^2$. We know that the equation $2 = a^2+b^2$ yields the solution, $(a,b) = (\pm 1, \pm 1)$. Hence substitution gives us $\pm a + \pm bi = \pm 1 + \pm i$. We then proceed to solve for $c$ and $d$.*

$$\begin{aligned} c+di &= \frac{1+3i}{a+bi} \\ &= \frac{1+3i}{\pm 1 + \pm i} \\ &= \frac{1+3i}{\pm 1 + \pm i} \cdot \frac{\pm 1 - \pm i}{\pm 1 - \pm i} \\ &= \frac{\pm 4 + \pm 2i}{2} \\ &= \pm 2 + \pm i. \end{aligned}$$

*Up to order of units, $a+bi = 1+i$, and $c+di = 2+i$.*

$$\therefore 1+3i = (a+bi)(c+di) = (1+i)(2+i).$$

We want to check which Gaussian integers of the form $a+bi$, where $b=0$ are irreducible. We focus only on ordinary integers that are already irreducible in $\mathbb{Z}$. The following proposition supports this claim.

**Proposition 4.2.3.** *Let $\gamma$ be reducible in $\mathbb{Z}$, then $\gamma$ is also reducible in $\mathbb{Z}[i]$.*

*Proof.* Suppose $\gamma$ is reducible in $\mathbb{Z}$ , then $\gamma = \alpha\beta$, where neither $\alpha$, nor $\beta$ is a unit. Taking the Gaussian integer norm we get, $N(\gamma) = N(\alpha)N(\beta)$. Since $\alpha$ and $\beta$ are non-units, $N(\alpha), N(\beta) \neq 1$, so neither $\alpha$ nor $\beta$ are associates of $\gamma$.

$\therefore \gamma$ is not irreducible in $\mathbb{Z}[i]$ if it is not irreducible in $\mathbb{Z}$. □

Take note that the converse of this proposition is not true. In other words, we cannot conclude that if an ordinary integer is irreducible in $\mathbb{Z}$, then it is also irreducible in $\mathbb{Z}[i]$. Let us take an example.

**Example 6.** *We choose the ordinary integer prime* $2$*. We know that* $2$ *is prime hence irreducible in* $\mathbb{Z}$*. We check if it is also irreducible in* $\mathbb{Z}[i]$*.*

*Let* $2 = (\pm a \pm bi)(\pm c \pm di)$*, where* $\pm a \pm bi$ *and* $\pm c \pm di$ *are Gaussian integers. Taking the norm we have,*

$$\begin{aligned} N(2) &= N[(a+bi)(c+di)] \\ (2)^2 &= N(a+bi)N(c+di) \\ 4 &= (a^2+b^2)(c^2+d^2) \\ 2 \cdot 2 &= (a^2+b^2)(c^2+d^2). \end{aligned}$$

*Let* $a^2+b^2 = 2$ *and* $c^2+d^2 = 2$*. The solution for the first equation then becomes,* $a = \pm 1$ *and* $b = \pm 1$*. Substituting these values into the equation* $2 = (a+bi)(c+di)$*, we get:*

$$\begin{aligned} c+di &= \frac{2}{a+bi} \\ &= \frac{2}{\pm 1 \pm i} \\ &= \frac{2}{\pm 1 \pm i} \cdot \frac{(\pm 1 \mp i)}{(\pm 1 \mp i)} \\ &= \left[\frac{2(\pm 1 \mp i)}{2}\right] \\ &= \pm 1 \mp i, \end{aligned}$$

*up to order of units,* $a+bi = 1+i$ *and* $c+di = 1-i$*. Therefore*

$$2 = (a+bi)(c+di) = (1+i)(1-i).$$

*The Gaussian integer* $1-i$ *is also irreducible since it is the conjugate of* $1+i$*, which we already proved to be irreducible.*

$\therefore 2$ *is a product of irreducibles of* $\mathbb{Z}[i]$*, and so it is not irreducible in* $\mathbb{Z}[i]$*, even though it is irreducible in* $\mathbb{Z}$*.*

The last example that is of great importance in Gaussian integer factorization is when $\alpha = 3$. This example will play a very important role in the classification of Gaussian primes later on.

**Example 7.** *Let* $3$ *be a Gaussian integer. We know that* $3$ *is prime, hence irreducible in* $\mathbb{Z}$*, so we want to investigate if it is still irreducible in* $\mathbb{Z}[i]$.

*Assume we can factorize* $3$ *into the product of Gaussian integers* $\pm a \pm bi$ *and* $\pm c \pm di$ *in the form* $3 = (\pm a \pm bi)(\pm c \pm di)$*. We want to check the state of this factorization by assessing it's norm as in previous examples.*

$$\begin{aligned} N(3) &= N[(\pm a \pm bi)(\pm c \pm di)] \\ (3)^2 &= N(\pm a \pm bi)N(\pm c \pm di) \\ 3 \cdot 3 &= (a^2 + b^2)(c^2 + d^2). \end{aligned}$$

*We then separate the equation into* $a^2 + b^2 = 3$ *and* $c^2 + d^2 = 3$*. However, no solution exists to either equation. Therefore by Remark* $7$*,* $3$ *is also irreducible in* $\mathbb{Z}[i]$.

Table 4.1 shows the few calculations we have compiled to show how factorization into irreducibles up to order of units and associates operates in $\mathbb{Z}[i]$. We shall reference some of these examples in the text.

## 4.3 When Unique Factorization Fails

We have seen that in the integral domain $\mathbb{Z}[i]$, not only is factorization into Gaussian irreducibles possible, but any such factorization is unique. We have also seen that this property is not only restricted to $\mathbb{Z}[i]$, as it also applies to every integral domain that satisfies the unique factorization property. We now extend the factorization theory to other integral domains using [7, 17].

**Corollary 4.3.0.1.** *The integral domain* $R = \mathbb{Z}[\sqrt{-5}]$ *is not a unique factorization domain.*

*Proof.* Let $R = \mathbb{Z}[\sqrt{-5}]$. $R$ is a ring with elements of the form $a + b\sqrt{-5}$, for some $a, b \in \mathbb{Z}$. We will borrow some properties from the arithmetic of $\mathbb{Z}[i]$ which we will not prove for $\mathbb{Z}[\sqrt{-5}]$, since the methodology is the same.

- The norm function $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$, defined by $N(a+b\sqrt{-5}) = a^2+5b^2$, exists.
- $N(\alpha\beta) = N(\alpha)N(\beta)$.
- If $\alpha|\beta$ in $\mathbb{Z}[\sqrt{-5}]$, then $N(\alpha)|N(\beta)$ in $\mathbb{Z}$.

Table 4.1: Gaussian Integer Factorization Table

| Gaussian Integer | Factorization | Irreducible | Reducible |
|---|---|---|---|
| $1+i$ | $(1)(1+i)$ | ✓ | × |
| $1+2i$ | $(1)(1+2i)$ | ✓ | × |
| $1+4i$ | $(1)(1+4i)$ | ✓ | × |
| $1+6i$ | $(1)(1+6i)$ | ✓ | × |
| $2+3i$ | $(1)(2+3i)$ | ✓ | × |
| $1+3i$ | $(1+i)(2+i)$ | × | ✓ |
| $1+5i$ | $(1+i)(3+2i)$ | × | ✓ |
| $4+2i$ | $(-i)(1+i)^2(2+i)$ | × | ✓ |
| $5+7i$ | $(1+i)(6+i)$ | × | ✓ |
| $6+2i$ | $-(1+i)^3(1+2i)$ | × | ✓ |
| 3 | $(1)(3)$ | ✓ | × |
| 7 | $(1)(7)$ | ✓ | × |
| 11 | $(1)(11)$ | ✓ | × |
| 19 | $(1)(19)$ | ✓ | × |
| 23 | $(1)(23)$ | ✓ | × |
| 31 | $(1)(31)$ | ✓ | × |
| 43 | $(1)(43)$ | ✓ | × |
| 47 | $(1)(47)$ | ✓ | × |
| 59 | $(1)(59)$ | ✓ | × |
| 2 | $(1+i)(1-i)$ | × | ✓ |
| 5 | $(1+2i)(1-2i)$ | × | ✓ |
| 13 | $(2+3i)(2-3i)$ | × | ✓ |
| 17 | $(1+4i)(1-4i)$ | × | ✓ |
| 29 | $(5+2i)(5-2i)$ | × | ✓ |
| 37 | $(1+6i)(1-6i)$ | × | ✓ |
| 41 | $(4+5i)(4-5i)$ | × | ✓ |
| 53 | $(2+7i)(2-7i)$ | × | ✓ |
| 61 | $(5+6i)(5-6i)$ | × | ✓ |

Notation: ✓ $= Yes$, × $= No$.

The units of $\mathbb{Z}[\sqrt{-5}]$ are the solutions to the equation $a^2+5b^2=1$, which are $(a,b)=(\pm 1,0)$. Therefore, the units of $\mathbb{Z}[\sqrt{-5}]$ are $\pm 1$. We will use Remark 7 to prove that the elements $2, 3, 1\pm\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Let $\alpha=2$. Taking the norm gives us $N(2)=4=(a^2+b^2)(c^2+5d^2)$. By Remark 7, we are

solving for the following equations.

$$(a^2 + 5b^2) = 2 \text{ and } (c^2 + 5d^2) = 2.$$

No solution exists to these two equations, therefore 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Let $\alpha = 3$. Taking the norm gives us $N(3) = 9 = (a^2+b^2)(c^2+5d^2)$. By Remark 7, we are solving for the following equations.

$$(a^2 + 5b^2) = 3 \text{ and } (c^2 + 5d^2) = 3.$$

No solutions exist to these two equations also. There 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Let $\alpha = 1 \pm b\sqrt{-5}$. Taking the norm gives us $N(1 \pm b\sqrt{-5}) = 6 = (a^2 + b^2)(c^2 + 5d^2)$. By Remark 7, we are solving for the following equations.

$$(a^2 + 5b^2) = 2 \text{ and } (c^2 + 5d^2) = 3.$$

These two equations have no solutions from our first two examples, where we had $\alpha = 2$, and $\alpha = 3$.

Choose $6 \in \mathbb{Z}[\sqrt{-5}]$, and factor it into a product of irreducibles of $\mathbb{Z}[\sqrt{-5}]$,

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

If $\mathbb{Z}[\sqrt{-5}]$ is a unique factorization domain, the two factorizations of 6 will be one factorization with a different multiplication of units, and reordering. We proved that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. We now want to see if 2 is prime in $\mathbb{Z}[\sqrt{-5}]$. Since $2|(1 + \sqrt{-5})(1 - \sqrt{-5})$, for 2 to be prime, either $2|(1 + \sqrt{-5})$, or $2|(1 - \sqrt{-5})$. To reiterate, if $\alpha|\beta$, then $N(\alpha)|N(\beta)$. Let $2|(1 + \sqrt{-5})$. Then $N(2) = 4$ must divide $N(1 + \sqrt{-5})$, where

$$\begin{aligned} N(1 + \sqrt{-5}) &= (1 + \sqrt{-5})(1 - \sqrt{-5}), \\ &= 1(1) - 1(\sqrt{-5}) + 1(\sqrt{-5}) - (\sqrt{-5})(\sqrt{-5}), \\ &= 1(1) - (\sqrt{-5})(\sqrt{-5}), \\ &= 1(1) - 1(-5) = 6. \end{aligned}$$

However, in $\mathbb{Z}$ we know that $4 \nmid 6$, so $N(2) \nmid N(1+\sqrt{-5})$, a contradiction. Hence $2 \nmid (1+\sqrt{-5})$. Next we assume that $2|(1 - \sqrt{-5})$. Using the same methodology, we find that $N(2) = 4 \nmid N(1 - \sqrt{-5}) = 6$. Hence $2 \nmid (1 - \sqrt{-5})$.

Therefore we can deduce that 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$, since $2|(1+\sqrt{-5})(1-\sqrt{-5})$, but $2 \nmid (1+\sqrt{-5})$, and $2 \nmid (1-\sqrt{-5})$. This implies that the factorizations $6 = 2 \cdot 3$ and $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two different factorizations of the same element in one integral domain, an indication that our ring is not a unique factorization domain. □

What this corollary has done is show us that while we can prove that every prime element is irreducible in an integral domain, not every irreducible element will be prime. This result is the consequence of having an integral domain that does not satisfy the unique factorization property.

## 4.4 Recovering Unique Factorization

We want to find a way to introduce the concept of uniqueness in integral domains where the unique factorization property fails. To do so we introduce new types of ideals called prime ideals. We want to prove that when unique factorization fails, we can effect uniqueness by factorizing the prime ideals uniquely using Artin [2].

**Proposition 4.4.1.** *Let $I$ be an ideal of a ring $R$. $I$ is called a prime ideal if $1 \notin I$, and if $\alpha\beta \in I$, then $\alpha \in I$ or $\beta \in I$.*

**Theorem 4.4.2.** *Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic field and $\mathcal{O}_K$ be the ring of integers in $K$. Every ideal $I$ of $\mathcal{O}_K$, excluding $0$ and $\mathcal{O}_K$ can be factored into a product of prime ideals. Furthermore, this factorization is unique up to ordering.*

See the proof in Trifkovic [25, p.80].

It will be convenient to identity the complex conjugate ideal corresponding to $I$ as follows (Artin [2, p. 420]):

$$\overline{I} = \{\overline{\alpha} : \alpha \in I\}.$$

As a lattice, $\overline{I}$ is obtained by reflecting the lattice $I$ about the real axis. It is clear that the conjugate of an ideal is again an ideal.

We want to use the above information to solve our factorization problem in the integral domain $\mathbb{Z}[\sqrt{-5}]$. We formulate the equation

$$(6) = (I_1 \cdot I_2)(I_3 \cdot I_4) = (I_1 \cdot I_3)(I_2 \cdot I_4).$$

By Proposition 3.1.3, if $\mathbb{Z}[\sqrt{-5}]$ was a UFD then we could find an element $\delta$ such that $\delta|2$ and $\delta|1+\sqrt{-5}$, which implies that $2 \subset (\delta)$ and $1+\sqrt{-5} \subset (\delta)$, where $(\delta)$ is a principal ideal. Since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, we cannot find any such element. Instead we form an ideal generated by the elements $2$ and $1+\sqrt{-5}$, which we shall denote by $(M) = (2, 1+\sqrt{-5})$.

By definition, $\overline{(M)} = (2, 1-\sqrt{-5})$. We then form another ideal $(N)$ generated by the elements 3 and $1+\sqrt{-5}$, denoted by $(N) = (3, 1+\sqrt{-5})$. By definition $\overline{(N)} = (3, 1-\sqrt{-5})$.

By Proposition 3.1.2, we are allowed to proceed with some manipulations to the given ideals.

$$(M\overline{M}) = (4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6).$$

We can see that $2|4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6$, hence $(M\overline{(M)}) \subset (2)$. Furthermore, $2 = 6-4$, hence $(2) \subset M\overline{M}$, which gives us, $(M\overline{(M)}) = (2)$.

Using the same method we see that $(N\overline{N}) = (9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6)$.

Again, $3|9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6$, hence $N\overline{N} \subset (3)$. Furthermore, $3 = 9-6$, hence $(3) \subset (N\overline{N})$. So we have, $(N\overline{N}) = (3)$.

We then look at the product $(MN)$. Our calculations lead us to,

$$(MN) = (6, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6).$$

We can see that $1+\sqrt{-5}|6, 3-3\sqrt{-5}, 3+3\sqrt{-5}$.

Hence $(MN) \subset (1+\sqrt{-5})$. Furthermore, $1+\sqrt{-5} = 3+3\sqrt{-5} - (2+2\sqrt{-5}) \in (MN)$. Therefore $(MN) = (1+\sqrt{-5})$

Using the same method we obtain $(\overline{MN}) = (1-\sqrt{-5})$.

Therefore,

$$(6) = (2)(3) = (M \cdot \overline{M})(N \cdot \overline{N}) = (M \cdot N)\overline{(M \cdot N)} = (1+\sqrt{-5})(1-\sqrt{-5})$$

We have successfully managed to write the ideal $(6)$ into a product of ideals. We next show that all these ideals are prime ideals. We will complete this task in the next Chapter.

# Chapter 5

# Modular Arithmetic In $\mathbb{Z}[i]$

## 5.1 Modular Arithmetic in $\mathbb{Z}$

Now that we have discussed the division of arbitrary elements in an integral domain $R$, we want to look at what happens when we divide the set itself, and consequently, the properties that occur using Judson [14]. To divide the set, we first need to assign a special relation that will separate the elements of the set, and allocate new subsets that each of the elements will occupy, according to the instructions of this governing relation. The following definition gives insight into this concept. We now introduce the concept of Modular Arithmetic in $\mathbb{Z}$.

**Definition 5.1.1.** *Let $R = \mathbb{Z}$ and let $\alpha, \beta$ be two ordinary integers and let $n \in \mathbb{N}$. We say $\alpha$ is congruent to $\beta$ modulo $n$, denoted by;*

$$\alpha \equiv \beta \text{ (mod n)},$$

*if $n|(\alpha - \beta)$, that is $\alpha - \beta = nk$, for some $k \in \mathbb{Z}$.*

**Theorem 5.1.1.** *$\equiv$ is an equivalence relation in $\mathbb{Z}$.*

*Proof.* Pick any arbitrary $\alpha, \beta, \gamma$ in $\mathbb{Z}$, and some $n \in \mathbb{N}$.

- $\alpha \equiv \alpha \pmod{n}$ since $\alpha - \alpha \equiv 0 \pmod{n} \Rightarrow 0 - 0 = n(0)$, for $0 \in \mathbb{Z}$.
- Assume $\alpha \equiv \beta \pmod{n}$, then $\alpha - \beta = nk$ for some $k \in \mathbb{Z}$.

  However if $\alpha - \beta = nk$, then $-(\beta - \alpha) = nk \Rightarrow (\beta - \alpha) = n(-k)$, for $-k \in \mathbb{Z}$.

  $\therefore \beta \equiv \alpha \pmod{n}$.

- Assume $\alpha \equiv \beta \pmod{n}$ and $\beta \equiv \gamma \pmod{n}$, then we can find some $r, s \in \mathbb{Z}$ such that $\alpha - \beta = nr$ and $\beta - \gamma = ns$.

  We want to show that $\alpha \equiv \gamma \pmod{n}$.

  $\alpha - \gamma = \alpha - \beta + \beta - \gamma = nr + ns = n(r + s)$. We know $r + s = t \in \mathbb{Z}$ since $r, s \in \mathbb{Z}$.

  $\therefore \alpha - \gamma = tn \Rightarrow \alpha \equiv \gamma \pmod{n}$.

Hence we can conclude that $\equiv$ forms an equivalence relation on $\mathbb{Z}$. □

**Definition 5.1.2.** *If $\alpha \equiv \beta$ (mod $n$), then we call $\beta$ a residue of $\alpha$ to modulus $n$.*

**Example 8.** *If we let $\alpha \equiv \beta$ (mod 2), then we have 2 equivalence classes under the relation $\equiv$.*

$$[0] = \ldots; -4; -2; 0; 2; 4; \ldots = S_1$$
$$[1] = \ldots; -5; -3; -1; 3; 5; \ldots = S_2.$$

*Therefore we say the equivalence classes $S_1$ and $S_2$ form a partition of the set $\mathbb{Z}$ under the relation $\alpha \equiv \beta$ (mod 2).*

When applying modular arithmetic, we are basically manipulating equations and changing how elements relate to each other in a ring. For example, we know that

$$5 \cdot 7 - 35 = 0 \text{ in } \mathbb{Z},$$

however, the equation

$$3 \cdot 5 - 4 = 0,$$

does not hold in $\mathbb{Z}$. To make it true, we can add a rule that $11 = 0$. This means we are reducing our answer mod 11.

In the ring $\mathbb{Z}$, if we choose an $\alpha$ in $\mathbb{Z}$, such that $\alpha = 0$, our answer no longer resides in $\mathbb{Z}$, but rather in a new structure denoted by $\mathbb{Z}/\alpha\mathbb{Z}$. We will learn about how these structures arise and their properties in the next subsection.

### 5.1.1 Factor Groups/Residue Classes

Let $R$ be a ring, and let $I$ be an ideal of $R$. Let $R/I$ represent the set of equivalence classes of $R$ under the equivalence relation $\sim$, denoted by $\alpha \sim \beta$ if $\alpha - \beta \in I$, for some $\alpha, \beta \in R$. Then the statement below follows by Judson [14].

**Theorem 5.1.2.** *$R/I = \{r+I | r \in R\}$ is a ring with addition defined by $(\alpha+I)+(\beta+I) = (\alpha+\beta)+I$, and multiplication defined by $(\alpha+I)(\beta+I) = (\alpha\beta)+I$, for $\alpha, \beta$ in $R/I$.*

*Proof.* Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in R$. If $\alpha_1 + I = \alpha_2 + I$ and $\beta_1 + I = \beta_2 + I$, then by definition, $\alpha_1 - \alpha_2 \in I$ and $\beta_1 - \beta_2 \in I$. We first show that the addition operation is well-defined. Take $\alpha_1 - \alpha_2$, and $\beta_1 - \beta_2$. Then,

$$(\alpha_1 - \alpha_2) + (\beta_1 - \beta_2) = (\alpha_1 + \beta_1) - (\alpha_2 + \beta_2) \in I,$$

which implies that $(\alpha_1+\beta_1)+I = (\alpha_2+\beta_2)+I$, and addition is well defined.

We now show that the multiplication operation is well defined. Taking $\alpha_1-\alpha_2$, and $\beta_1 - \beta_2$ again, we have,

$$\begin{aligned} \alpha_1\beta_1 - \alpha_2\beta_2 &= \alpha_1\beta_1 - \alpha_1\beta_2 - \alpha_1\beta_2 - \alpha_2\beta_2, \\ &= \alpha_1(\beta_1 - \beta_2) - (\alpha_1 + \alpha_2)\beta_2 \in I. \end{aligned}$$

Hence $\alpha_1\beta_1 + I = \alpha_2\beta_2 + I$, and multiplication is well defined in $R/I$. We then use Theorem 2.0.1 complete the proof.

- $(\alpha + I) + (\beta + I) = (\alpha + \beta) + I = (\beta + \alpha) + I = (\beta + I) + (\alpha + I)$.
- $[(\alpha+I)+(\beta+I)]+(\gamma+I)) = [(\alpha+\beta)+I]+(\gamma+I) = (\alpha+\beta+\gamma)+I = (\alpha + I) + (\beta + \gamma + I) = (\alpha + I) + [(\beta + I) + (\gamma + I)]$.
- There exists an element $0_R + I$, such that $(\alpha + I) + 0_R + I = \alpha + I$.
- There exists an element $[(-\alpha)+I]$ such that $[(-\alpha)+I]+(\alpha+I) = 0_R+I$.
- $(\alpha + I)[(\beta + I)(\gamma + I)] = (\alpha + I)[(\beta\gamma + I)] = \alpha(\beta\gamma) + I = (\alpha\beta)\gamma + I = (\alpha\beta + I)(\gamma + I) = [(\alpha + I)(\beta + I)](\gamma + I) = [(\alpha + I)(\beta + I)](\gamma + I)$.
- $(\alpha + I)[(\beta + I)(\gamma + I)] = (\alpha + I) + [(\beta + \gamma) + I] = \alpha(\beta + \gamma) + I = [(\alpha\beta+\alpha+\gamma)+I] = (\alpha\beta+I)(\alpha\gamma+I) = (\alpha+I)(\gamma+I)+(\alpha+I)(\gamma+I)$.

Therefore we can conclude that $R/I$ is a ring.

□

**Corollary 5.1.2.1.** *Let $n \in \mathbb{Z}$, then $\mathbb{Z}/n\mathbb{Z}$ is a ring.*

*Proof.* Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$, then by the previous theorem, $\mathbb{Z}/n\mathbb{Z}$ is a ring. □

**Definition 5.1.3.** *We denote the equivalence classes of $\mathbb{Z}$ under the equivalence relation $\equiv$ by $\mathbb{Z}/n\mathbb{Z}$. This set is called the set of integers modulo $n$.*

Since we only consider integral domains in this paper, it is important to clarify which aspect of the ring $\mathbb{Z}/n\mathbb{Z}$ we will work with using Ho [13].

**Theorem 5.1.3.** *Let $R$ be the integral domain $\mathbb{Z}$, and let $\mathbb{Z}/n\mathbb{Z}$ be the set of equivalence classes of $R$ under $\equiv$, then $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if $n$ is an ordinary integer prime.*

*Proof.* $\Rightarrow$ Choose $n$ not prime. Then $n \equiv \alpha\beta$, where $\alpha \not\equiv 0$ and $\beta \not\equiv 0$ are non-units. Therefore $\alpha\beta \equiv 0$ in the ring $\mathbb{Z}/n\mathbb{Z}$.

$\Leftarrow$ Let $n$ be prime. By Definition 3.1.6, $n|\alpha\beta$ if and only if $n|\alpha$ or $n|\beta$. Therefore $\alpha \equiv 0$, or $b \equiv 0$ in the ring $\mathbb{Z}/n\mathbb{Z}$.

□

**Example 9.** *Take the ring of integers modulo 15, i.e $\mathbb{Z}/15\mathbb{Z}$.*

$$\mathbb{Z}/15\mathbb{Z} = \{\alpha : \alpha \in \mathbb{Z}/15\mathbb{Z}\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}.$$

*We know that $3 \not\equiv 0$ and $5 \not\equiv 0$, however*

$$3 \cdot 5 \equiv 15 \equiv 0 \text{ (mod 15)}.$$

*$\therefore 3$ and $5$ are zero divisors. In-fact, $[3] \cdot [5] \equiv 0$ (mod $15$). As a result, the ring $\mathbb{Z}/15\mathbb{Z}$ is not an integral domain.*

*We have to note that we only choose $n$ to be prime because of the concept of cancellation in the ring $\mathbb{Z}/n\mathbb{Z}$. Going back to our ring $\mathbb{Z}/15\mathbb{Z}$, we have*

$$3 \cdot 1 \equiv 3 \cdot 6 \text{ (mod } 15),$$

*but when considering equivalence classes, $[1] \not\equiv [6]$, hence $1 \not\equiv 6$ in $\mathbb{Z}/15\mathbb{Z}$. Consequently, the cancellation property fails.*

In that case, we are only going to consider $\mathbb{Z}/p\mathbb{Z}$, for an ordinary integer $p$, which is a field since when $p$ is an integer prime, every element in $\mathbb{Z}/p\mathbb{Z}$ has an inverse.

## 5.2 Utilizing Modular Arithmetic in $\mathbb{Z}[i]$

We have already proved that modular arithmetic is an equivalence relation in the ring of integers. We now want to show how modular arithmetic in $\mathbb{Z}[i]$ is closely linked to the modular arithmetic of $\mathbb{Z}$, the same way division in $\mathbb{Z}$ has close ties to division in $\mathbb{Z}[i]$.

**Definition 5.2.1.** *Let $a+bi, m+ni, r+si$ be Gaussian integers. We say*

$$a+bi \equiv m+ni \text{ (mod } r+si),$$

*in $\mathbb{Z}[i]$, if and only if $r+si|(a+bi)-(m+ni)$. That is $r+si$ divides $(a-m)+(b-n)i$.*

**Example 10.** *Let $a+bi \equiv 8+11i$, $m+ni \equiv 2+3i$, and $r+si \equiv 3+4i$. We want to check if the congruence is true:*

$$a+bi \equiv m+ni \text{ (mod } r+si).$$

*We want to see if we can find a Gaussian integer $u+vi$ such that,*

$$(a-m)+(b-n)i = (u+vi)(r+si).$$

*Firstly, $(a-m)+(b-n)i = (8-2)+(11-3)i = 6+8i$. Hence, $6+8i = (u+vi)(3+4i)$. Solving for $u+vi$ we get,*

$$u+vi = \frac{6+8i}{3+4i} = 2.$$

*Since $2 \in \mathbb{Z}[i]$, we can conclude that $2+3i|(a-m)+(b-n)i = (8-2)+(11-3)i = 6+8i$, and therefore,*

$$8+11i \equiv 2+3i \text{ (mod } 3+4i).$$

If we eliminate the coefficients of the imaginary parts from the Modular arithmetic for $\mathbb{Z}[i]$, we get the normal Modular arithmetic for $\mathbb{Z}$. Gaussian integer modular arithmetic preserves the integer modular arithmetic, and so the next statement is justified.

**Theorem 5.2.1.** *Let $\alpha, \beta$ and $\gamma$ be elements of the ring $\mathbb{Z}$. Then $\alpha \equiv \beta$ (mod $\gamma$) in the ring $\mathbb{Z}$ if and only if $\alpha \equiv \beta$ (mod $\gamma$) in the ring $\mathbb{Z}[i]$.*

As in $\mathbb{Z}$, the set of equivalence classes of $\mathbb{Z}[i]$ under $\equiv$ is the ring $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$. We can also denote this ring as $\mathbb{Z}[i]/(\alpha)$, where $(\alpha)$ represents the principal ideal generated by the element $\alpha$. Similarly, for the equivalence classes $\mathbb{Z}[i]/(\alpha)$, we are only going to consider the cases where $\alpha$ is prime in $\mathbb{Z}[i]$. However, since we have not explicitly stated what primes in $\mathbb{Z}[i]$ look like, we can utilize the fact that $\mathbb{Z}[i]$ is a UFD, hence every irreducible is prime. Consequently, we will let $\alpha$ be a Gaussian irreducible.

We will look at examples of how we can use modular arithmetic in $\mathbb{Z}[i]$ (found in Artin [2]). We first use Judson [14] to introduce the following definitions for rings $R$ and $R'$.

**Definition 5.2.2.** *A $\theta : R \to R'$ is called a one-to-one map if*

$$\theta(\alpha) = \theta(\beta) \text{ implies that } \alpha = \beta,$$

*for $\alpha, \beta$ in $R$.*

**Definition 5.2.3.** *If $\theta : R \to R'$ and $\theta(R) = R'$, then $\theta$ is called an onto or surjective map.*

**Definition 5.2.4.** *The map $\theta : R \to R'$ is called a homomorphism if for all $\alpha, \beta \in R$:*

- $\theta(\alpha + \beta) = \theta(\alpha) + \theta(\beta)$.
- $\theta(\alpha\beta) = \theta(\alpha)\theta(\beta)$.

**Definition 5.2.5.** *Let $\theta : R \to R'$. The kernel of a homomorphism is defined to be the set*

$$ker(\theta) = \{r \in R | \theta(r) = 0\}.$$

**Definition 5.2.6.** *A map $\theta : R \to R'$ that is a one-to-one and onto homomorphism is called an isomorphism. We say $R$ is isomorphic to $R'$ and denote this as,*

$$R \cong R'.$$

**Example 11.** *Let $1 + i \equiv 0$ in $\mathbb{Z}[i]$. We work in the ring $\mathbb{Z}[i]/(1 + i)$.*

*Since $1 + i \equiv 0$, we have $1 \equiv -i$. If we multiply both sides of the equation by $-i$ we get $-i \equiv -1$. But we said $1 \equiv -i$, hence $1 \equiv -1$, which implies that $1 + 1 \equiv 0$, therefore $2 \equiv 0$. The equivalences classes for both rings are $[0]$ and $[1]$. From this example we claim, and will prove that $\mathbb{Z}[i]/(1 + i)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

**Example 12.** *For this example consider the integer* $1+3i$ *which is not irreducible in* $\mathbb{Z}[i]$ *as per table* 4.1. *We let* $1+3i \equiv 0$*, and work in the ring* $\mathbb{Z}[i]/(1+3i)$*. Since* $1+3i \equiv 0$*, we can let* $1 \equiv -3i$*. If we multiply both sides of the equation by* $i$ *we get* $i(1) \equiv i(-3i)$*, and after multiplication,* $i \equiv 3$*. We then substitute* $i \equiv 3$ *in the equation* $1 \equiv -3i$ *to get* $1 \equiv -3(3)$*, which implies that* $1 \equiv -9$*, and finally,* $10 \equiv 0$*. We claim, and will prove that the ring* $\mathbb{Z}/1+3i\mathbb{Z}$ *is isomorphic to the ring* $\mathbb{Z}/10\mathbb{Z}$*.*

To prove that $\mathbb{Z}/1+3i\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}/2\mathbb{Z}$, we invoke the following general result. Our proof is taken from the excellent account by Dresden-Dymacek [10].

Before stating the theorem, we recall some intuitive facts.

**Fact 1**. We have

$$\mathbb{Z}[i]/(a+bi) \cong \mathbb{Z}[i]/(-a-bi) \cong \mathbb{Z}[i]/(-b+ai) \cong \mathbb{Z}[i]/(b-ai).$$

This follows from the fact that the units of $\mathbb{Z}$ are $1, -1, i, -i$, and these force the equalities of ideals $(b+ai) = (-a-bi) = (-b+ai) = (b-ai)$.

**Fact 2**. The following isomorphisms are intuitive derivations from relations in the ring $\mathbb{Z}$:

$$\mathbb{Z}[i]/(0) \cong \mathbb{Z}[i] \qquad \text{and} \qquad \mathbb{Z}[i]/(1) \cong \{0\}.$$

**Theorem 5.2.2.** *If* $\gcd(a,b) = 1$*, then*

$$\mathbb{Z}[i]/(a+bi) \cong \mathbb{Z}_{a^2+b^2}.$$

*Proof.* Because of **Fact 1** we may assume that $a > 0, b > 0$. Note that $\gcd(a,b) = 1 \implies \gcd(b, a^2+b^2) = 1$, so $b^{-1}$ exists in $\mathbb{Z}_{a^2+b^2}$ (where $b$ stands for $[b]_{a^2+b^2}$). We have

$$a^2 + b^2 \equiv 0 \pmod{a^2+b^2} \implies a^2 \equiv -b^2 \pmod{a^2+b^2}$$

$$\implies (ab^{-1})^2 \equiv -1 \pmod{a^2+b^2}.$$

Now define $\theta : \mathbb{Z}[i] \to \mathbb{Z}a^2 + b^2$ by $\theta(x+yi) = x - (ab^{-1})y$ modulo $a^2+b^2$. It is clear that $\theta$ is a surjective homomorphism with respect to addition. We verify only the preservation of multiplication.

Let $\alpha = x + yi, \beta = w + zi \in \mathbb{Z}[i]$. Then

$$\begin{aligned}
\theta(\alpha) \cdot \theta(\beta) &= \theta(x + yi)\theta(w + zi) \\
&= \theta(x + ab^{-1}y)\theta(w + ab^{-1}z) \\
&= (xw) + a^2b^{-2}(yz) - ab^{-1}(xz + yw) \\
&= (xw - yz) - ab^{-1}(xz + yw) \\
&= \theta((xw - yz) + (xz + yw)) \\
&= \theta((x + yi) \cdot (w + zi)) \\
&= \theta(\alpha \cdot \beta).
\end{aligned}$$

This shows that $\theta$ preserves multiplication. In addition, since $\theta(a + bi) = a - ab^{-1}b = 0$, it follows that $(a + bi) \subseteq \ker(\theta)$.

Let $c+di \in \ker(\theta)$ and let $c+di = (a+bi)(x+yi)$, where $x$ and $y$ are rational numbers. Since $= \theta(a + bi) = a - ab^{-1}b$, we have that $0 = bc - ad$, which by the division rule for complex numbers, makes $y$ an integer. Multiplying through by $ab$ gives

$$0 = bc - ad \implies 0 = ab^2c - a^2bd \implies 0 = ac - a^2b^{-2}bd.$$

Thus from $(ab^{-1})^2 \equiv -1$, we get $0 \equiv ac + bd$; so $x$ is also an integer. We deduce that $\ker(\theta) \subseteq (a+bi)$, which implies that $\ker(\theta) = (a+bi)$. Hence it follows from the First Isomorphism Theorem that $\mathbb{Z}[i]/(a + bi)$ is isomorphic to $\mathbb{Z}_{a^2+b^2}$. □

**Corollary 5.2.2.1.** *We have*

*(i)* $\mathbb{Z}/1 + 3i\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}$.

*(ii)* $\mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}/2\mathbb{Z}$.

*Proof.* These results follow at once from Theorem 5.2.2 using the well-known isomorphism $\mathbb{Z}/a\mathbb{Z} \cong \mathbb{Z}_a$ for any positive integer $a$.

(i) Set $a = 1,\ b = 3$ in Theorem 5.2.2.

(ii) Set $a = b = 1$ in Theorem 5.2.2. □

We can use this information to support the fact that the ideals $(M) = (2, 1 + \sqrt{-5}), (\overline{M}) = (2, 1 - \sqrt{-5}), (N) = (3, 1 + \sqrt{-5})$ and $(\overline{N}) = (3, 1 - \sqrt{-5})$ are prime ideals in $\mathbb{Z}[\sqrt{-5}]$. Milne [17, p.12] expands on this.

## 5.3 Modular Arithmetic on Squares

A very important application of modular arithmetic is on integer squares. To understand how integer squares operate we go back to the knowledge of odd and even integers. We know that an ordinary integer $\alpha$ that is even has the form $\alpha = 2k$, for some $k$ in $\mathbb{Z}$, while an odd ordinary integer $\beta$ can be written in the form, $\alpha = 2k + 1$, for some $k$ in $\mathbb{Z}$. If we square an even integer $\alpha$, we get $(\alpha)^2 = (2k)^2 = 4k^2$. Applying the division algorithm tells us that, every even square will always be divisible by $4$ without a remainder, and since we can let $k$ be any ordinary integer, this accounts for every even square possible. Therefore every even square satisfies the property

$$\alpha^2 \equiv 0 \text{ (mod 4)}.$$

Taking the square of an odd integer $\beta$ gives us the equation,

$$(\beta)^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 = 4m + 1,$$

where $k^2 + k = m$, for some $m \in \mathbb{Z}$. Applying the division algorithm, we observe that if we divide $\beta^2$ by $4$ we will always get 1 as a remainder. Therefore the following property follows for odd squares.

$$\beta^2 \equiv 1 \text{ (mod 4)}.$$

**Proposition 5.3.1** (The properties of squares)**.** *Let $R = \mathbb{Z}$ be an integral domain, and let $\alpha^2$ be an even square in $R$, while $\beta^2$ is an odd square in $R$. Then we have the following conditions.*

- $\alpha^2 + \alpha^2 \equiv \alpha^2$ (mod 4).
- $\beta^2 + \beta^2$ (mod 4) is not a square.
- $\alpha^2 + \beta^2 \equiv \beta^2$ (mod 4).

*Proof.*

$$\begin{aligned} \alpha^2 + \alpha^2 &\equiv 0 + 0 \quad (mod 4) \equiv 0 \quad (mod 4). \\ \beta^2 + \beta^2 &\equiv 1 + 1 \quad (mod 4) \equiv 2 \quad (mod 4). \\ \alpha^2 + \beta^2 &\equiv 0 + 1 \quad (mod 4) \equiv 1 \quad (mod 4). \end{aligned}$$

□

### 5.3.1 Modular Arithmetic on Irreducible Polynomials

We can also apply modular arithmetic to irreducible polynomials, which will be defined below using Artin [2].

**Definition 5.3.1.** *A polynomial $p(x)$ which has co-efficients in a Field $F$ is called an irreducible polynomial if it is not constant, and if the only divisors of $p(x)$ of lower degree in $F(x)$ are constants.*

For a prime $p$ in $\mathbb{N}$, we consider the equation,

$$x^2 \equiv \alpha(mod \quad p) \tag{5.1}$$

When $p$ is relatively small, we can solve this equation easily by hand. However, for large $p$, we want to use a method that is very fast and easy to apply.

Again we only consider our reduction mod $p$, where $p$ is prime because if it is not, then we encounter some problems. Let us look at an example.

**Example 13.** *Going back to the ring $R = \mathbb{Z}/15\mathbb{Z}$, let $x^2 - 1$ be a polynomial from the ring $R[x]$. The equations*

$$x^2 - 1 = (x - 1)(x + 1) = (x + 4)(x - 4)$$

*are true in $\mathbb{Z}/15\mathbb{Z}$ since $x^2 - 16 \equiv (x^2 - 1)$ (mod 15).*

*This means the factorization of the polynomial $x^2 - 16$ into irreducible polynomials will not be unique. The implication of this statement is that when dealing with a ring that is not an integral domain, more that two solutions will exist for a quadratic equation. Consequently, for higher order equations even more solutions will exist. This is why we only operate in integral domains, because in integral domains we are sure that all the solutions we will find are the only solutions possible. No other solutions will exist outside of those.*

When $p$ is relatively small, solving the equation $x^2 \equiv \alpha \pmod{p}$ can done by hand as shown in the table below.

Table 5.1: Reduction Table For 11

| $x$ | 0 | $\pm 1$ | $\pm 2$ | $\pm 3$ | $\pm 4$ | $\pm 5$ |
|---|---|---|---|---|---|---|
| $x^2 \pmod{11}$ | 0 | 1 | 4 | 9 | 5 | 3 |

In this case we see that $x = 2$ is a solution since $x^2$ is a square.

For large $p$ We introduce the Legendre symbol using Murty [18] as defined below.

**Definition 5.3.2.** *Let $p$ be an odd prime in the integral domain $\mathbb{N}$, and $\alpha \in \mathbb{Z}$. The Legendre symbol denoted by $\left(\frac{\alpha}{p}\right)$ is defined by;*

$$\left(\frac{\alpha}{p}\right) = \begin{cases} 1, & \text{if Equation 5.1 has a solution} \\ -1, & \text{if Equation 5.1 has no solution} \end{cases}$$

*In the case where $p$ divides $\alpha$ then $\left(\frac{\alpha}{p}\right) = 0$.*

From the reduction table we can see that $\left(\frac{2}{7}\right) = 1$, $\left(\frac{4}{7}\right) = -1$, and $\left(\frac{14}{7}\right) = 0$.

We will prove a very important property of the Legendre symbol which we shall utilize in the next chapter using Fermat's Little Theorem, and Euler's Criterion which we will define below.

**Proposition 5.3.2** (Fermat's Little Theorem)**.** *Let $p$ be an odd prime in $\mathbb{Z}$. Then for $x \not\equiv 0$ in $\mathbb{Z}$ we have $x^{p-1} \equiv 1$ (mod p).*

**Proposition 5.3.3** (Euler's Criterion)**.** *Let $p \in \mathbb{Z}$ be an odd prime. Then*

$$\alpha^{(p-1)/2} \equiv \left(\frac{\alpha}{p}\right) \text{ (mod } p\text{).}$$

**Proposition 5.3.4.** *Let $p \in \mathbb{Z}$ be an odd prime. Then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1$ (mod 4).*

*Proof.* $\Rightarrow$ Let $x$ in $\mathbb{Z}$ such that the equation $x^2 \equiv -1 \pmod{p}$ has a solution. Since $p$ is odd, we have $p \not\equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Suppose the latter, i.e. $p = 4r + 3$. Then,

$$\begin{aligned} x^{p-1} &\equiv x^{(4r+3)-1} \\ &\equiv x^{4r+2} \\ &\equiv (x^2)^{2r+1}. \end{aligned}$$

But $(x^2)^{2r+1} = (-1)^{2r+1} \pmod{p} \equiv -1 \pmod{p}$, contradicting Fermat's Little Theorem. Therefore $p = 4r + 1$.

$\Leftarrow$ Using Euler's criterion, let $\alpha = -1$. Then,

$$(-1)^{(p-1)/2} \equiv \left(\frac{-1}{p}\right).$$

Let $p \equiv 1 \pmod 4$, then $p = 4r+1$, $r \in \mathbb{Z}$. We have $(-1)^{(p-1)/2} = (-1)^{[(4r+1)-1]/2} = (-1)^{2r} = 1$. Therefore $1 \equiv \left(\frac{-1}{p}\right)$. However, $\left(\frac{-1}{p}\right)$ is either the integer $1$ or the integer $-1$, therefore $\left(\frac{-1}{p}\right) = 1$ as desired.

□

# Chapter 6

# Gaussian Primes

## 6.1 Pure Gaussian Primes

For this chapter we study Gaussian integer primes using the information we gathered on ordinary integer primes and Gaussian irreducibles under the factorization chapter. Corollary $4.2.2.1$ states that, Gaussian irreducibles are elements that only have 8 divisors, and since we have established that $\mathbb{Z}[i]$ is a UFD, all Gaussian irreducibles are Gaussian primes, and from that statement we can define prime elements in $\mathbb{Z}[i]$.

**Definition 6.1.1.** *A Gaussian integer $\alpha = a + bi$ is called a pure Gaussian prime if $a, b \neq 0$, and $\alpha$ only has $8$ divisors, viz;*

$$\pm 1, \pm i, \pm \alpha, \pm i\alpha.$$

**Theorem 6.1.1** (Conrad [9])**.** *Let $a + bi$ be a Gaussian integer, and $p$ be an ordinary integer. If $p$ is prime in $\mathbb{Z}$, and $N(a + bi) = p$, then $a + bi$ is prime in $\mathbb{Z}[i]$.*

*Proof.* Let a+bi be a Gaussian integer with $N(a + bi) = p$, where $p$ is prime in $\mathbb{Z}$. Choose $(a + bi) = (m + ni)(r + si)$ to be a factorization of $a + bi$, where $m + ni, r + si$ are Gaussian integers. Taking the norm of the factorization we get $N(a + bi) = N[(m + ni)(r + si)]$, using the multiplicativity of the norm, $N(a + bi) = N(m + ni)N(r + si)$, which gives us $p = N(m + ni)(r + si)$.

We know that $N(m + ni) \in \mathbb{Z}$, and $N(r + si) \in \mathbb{Z}$, and since $p$ is prime in $\mathbb{Z}$, either $N(m + ni) = 1$, or $N(r + si) = 1$. By the definition of units in $\mathbb{Z}[i]$, either $m + ni$ or $r + si$ is a unit, which implies that $a + bi$ is prime.

□

**Corollary 6.1.1.1.** *Suppose $\alpha = a + bi$ is a pure Gaussian integer prime, then the following are true.*

- *$u\alpha$, for all $u \in U(\mathbb{Z}[i])$, is a Gaussian prime.*
- *$\overline{\alpha}$ is a Gaussian prime.*

*Proof.* This proof follows from the fact that, a pure Gaussian integer prime shares the same norm with it's conjugate, and all it's associates. This also proves Corollary 4.2.2.1 and shows the interplay between conjugates, irreducibility and primality. □

From the factorization table (Table $4.1$) we can see that Theorem $6.1.1$ applies to the elements $1 + i, 1 + 2i, 1 + 4i, 1 + 6i, 2 + 3i, 2 + 7i, 4 + 5i, 5 + 2i, 5 + 6i$, which all happen to be irreducible, proving that indeed $\mathbb{Z}[i]$ is a UFD.

## 6.2 Gaussian Integer primes of the form a+bi, a=0 and b=0

For this section, we want to see which ordinary prime integers carry their primality from $\mathbb{Z}$ to $\mathbb{Z}[i]$. We will focus on integers that are already prime in $\mathbb{Z}$, because if a non-prime ordinary integer is not irreducible in $\mathbb{Z}$, it will not be irreducible in $\mathbb{Z}[i]$, and therefore it cannot be prime in $\mathbb{Z}[i]$. We want to see if Theorem $6.1.1$ holds for a Gaussian integer $a + bi$, where $b = 0$ and $a$ is a prime $p$ in $\mathbb{N}$. Below is an example where $N(p) = p^2$.

**Example 14.** *Let $3$ be a Gaussian integer. We have proven that $3$ is a Gaussian irreducible in example $7$. We can then conclude that it is also a Gaussian prime since $\mathbb{Z}[i]$ is a UFD. However for this to be true according to Theorem $6.1.1$, $N(3)$ will have to be a prime in $\mathbb{N}$. But $N(3) = 9$ which is not an ordinary integer prime.Therefore we have confirmed that Theorem $6.1.1$ does not hold in general for $a + bi$, where $b = 0$. It is reserved for pure Gaussian integers.*

To reiterate, Theorem $6.1.1$ says if $N(a+bi) = p$, for some prime $p$ in $\mathbb{Z}$, then the pure Gaussian integer $a + bi$ is a Gaussian prime. However, if we start from the bottom up we get,

$$p = a^2 + b^2 = (a + bi)(a - bi) = N(a + bi).$$

This implies that any ordinary prime $p$, that is the norm of a Gaussian prime $p$ cannot be prime in $\mathbb{Z}[i]$, since from the statement we can see that $p = (a + bi)(a - bi)$, which is a product of prime Gaussian integers. From this information we can formulate the following statements.

**Theorem 6.2.1.** *Let $p \in \mathbb{N}$ be prime. If $p$ is reducible in $\mathbb{Z}[i]$, then $p$ can be expressed in the form $p = a^2 + b^2$.*

*Proof.* Suppose $p \in \mathbb{N}$ is reducible in $\mathbb{Z}[i]$, then

$$p = (a + bi)(c + di),$$

where $a + bi$ and $c + di$ are Gaussian primes. Taking the norm,

$$\begin{aligned} N(p) &= N[(a + bi)(c + di)] \\ p^2 &= N(a + bi)N(c + di) \\ p \cdot p &= N(a + bi)N(c + di). \end{aligned}$$

Then $N(a + bi) = p$ since $N(a + bi), N(c + di) > 1$. $N(a + bi) = p^2$ yields a contradiction, therefore $a^2 + b^2 = p$. □

**Theorem 6.2.2.** *Let $p \in \mathbb{N}$ be prime in $\mathbb{Z}$. If $p = a^2 + b^2$, then $p$ is not prime in $\mathbb{Z}[i]$.*

*Proof.* Let $p \in \mathbb{N}$ be a prime in $\mathbb{Z}$. Then $p$ can be factored into

$$p = a^2 + b^2 = (a + bi)(a - bi) \text{ in } \mathbb{Z}[i].$$

By Theorem 6.1.1, we know that both $a + bi$ and $a - bi$ are Gaussian primes. Hence, if $p = a^2 + b^2$ is prime, then $p$ is reducible in $\mathbb{Z}[i]$. □

**Theorem 6.2.3.** *Let $p \in \mathbb{N}$ be prime in $\mathbb{Z}$. If $p$ is reducible in $\mathbb{Z}[i]$, then it can only be factored into a maximum of two Gaussian primes.*

*Proof.* Let $p = \alpha_1 \cdots \alpha_k$, for $k \in \mathbb{N}$. Taking the norm,

$$\begin{aligned} N(p) &= N(\alpha_1 \cdots \alpha_k) \\ p^2 &= N(\alpha_1)N(\alpha_2) \cdots N(\alpha_k). \end{aligned}$$

By factorization we have,

$$p \cdot p \cdot 1 \cdots 1 = N(\alpha_1)N(\alpha_2) \cdots N(\alpha_k).$$

Therefore,

$$p = N(\alpha_1), p = N(\alpha_2), 1 = N(\alpha_3), \ldots, 1 = N(\alpha_3),$$

and $\alpha_3, \ldots, \alpha_k, k \in \mathbb{N}$ are units of $\mathbb{Z}[i]$. □

An example of a prime $p \in \mathbb{Z}$ that fails to be prime in $\mathbb{Z}[i]$ is $p = 2$. We know that $2 = 1^2 + 1^2$. In-fact we proved 2 is not irreducible in $\mathbb{Z}[i]$ since $2 = (1 + i)(1 - i)$ in Example 6. This proof solidifies the fact that since $\mathbb{Z}[i]$ is a UFD, no Gaussian integer that is reducible can possibly be prime. Using the factorization table 4.1 we can also look at other examples of integer primes that fail to be prime in $\mathbb{Z}[i]$, being

$$5, 13, 17, 29, 37, 41, 53, 61,$$

which reiterates what we have discussed so far. We want to check the difference between integers that can be written as the sum of two squares, and those that cannot. We know that no prime integer $p$ is a square, and except when $p = 2$, $p$ is odd. Hence we can conclude that, if $p = a^2 + b^2$, then

$$a = 2k \text{ and } b = 2k + 1,$$

and

$$\begin{aligned} p &= a^2 + b^2 \\ &= (2k)^2 + (2k + 1)^2 \\ &= 4k^2 + 4k^2 + 4k + 1 \\ &= 8k^2 + 4k + 1 \\ &= 4(2k^2 + k) + 1. \end{aligned}$$

Therefore if we let $(2k^2 + k) = n$, we can deduce that $p = 4n + 1$ or $p \equiv 1 \pmod 4$. We use Stillwell [24] for the next statement.

**Theorem 6.2.4.** *Let $p \in \mathbb{N}$ be an ordinary integer prime. Then $p$ can be written as $p = a^2 + b^2$, for some $a, b \in \mathbb{Z} \Leftrightarrow p \equiv 1$ (mod 4).*

*Proof.* $\Rightarrow$ Let $p = a^2 + b^2$, for some $a, b \in \mathbb{Z}$. Then from the working above, $p = 4n + 1$, for some $n \in \mathbb{Z}$, which implies that $p \equiv 1 \pmod 4$.

$\Leftarrow$ Assume $p \equiv 1 \pmod 4$. Then by Proposition 5.3.4, $\left(\dfrac{-1}{p}\right) = 1$ meaning that we can find an integer $x$ in $\mathbb{Z}$ such that $x^2 \equiv -1 \pmod p$. By modulo definition, $p|x^2 + 1$. Let $x^2 + 1 = (x + i)(x - i)$, hence $p|(x + i)(x - i)$ in $\mathbb{Z}[i]$.

By Euclid's Lemma for Gaussian integers [Lemma 4.2.1], if $p$ is prime in $\mathbb{Z}[i]$, then either $p|(x + i)$ or $p|(x - i)$. But,

$$\frac{x}{p} \pm \frac{1}{p}i \notin \mathbb{Z}[i], \text{ since } \pm\frac{1}{p} \notin \mathbb{Z}[i].$$

Hence $p$ is reducible in $\mathbb{Z}[i]$ instead. Assume $p = (a+bi)(c+di)$, where $a+bi$ are $c+di$ are Gaussian primes. Taking the norm we get,

$$\begin{aligned} N(p) &= N[(a+bi)(c+di)] \\ p^2 &= N(a+bi)N(c+di) \\ p \cdot p &= N(a+bi)N(c+di), \end{aligned}$$

$N(a+bi) = p$, then $p = (a+bi)(a-bi) = a^2 + b^2$. □

**Corollary 6.2.4.1.** *Let $p \in \mathbb{Z}$ be prime, with $p \equiv 1$ (mod 4), then $p$ can be factored into a product of Gaussian primes in $\mathbb{Z}[i]$.*

*Proof.* The proof follows from the fact that when $p \equiv 1 \pmod 4$, then $p = a^2 + b^2 = (a+bi)(a-bi)$ which is a product of pure Gaussian primes. □

**Corollary 6.2.4.2.** *Let $p \in \mathbb{Z}$ be prime. If $p \equiv 1$ (mod 4), then $p$ is not prime in $\mathbb{Z}[i]$.*

*Proof.* The proof follows directly from the last Corollary above. □

From this information we can deduce that if $p \equiv 1 \pmod 4$, then $p$ cannot be prime in $\mathbb{Z}[i]$, but what about the remaining ordinary integer primes? We look at the case $p \in \mathbb{Z}$ when $p \equiv 2, 3 \pmod 4$. For $p \equiv 2 \pmod 4$ we only have the prime $p = 2$. We now focus on the case when $p \equiv 3 \pmod 4$. We claim that if $p \equiv 3 \pmod 4$ for some $p \in \mathbb{N}$ which is prime in $\mathbb{Z}$, then $p$ is prime in $\mathbb{Z}[i]$. We explore this claim.

**Theorem 6.2.5.** *Let $p \in \mathbb{N}$ be prime in $\mathbb{Z}$. If $p \equiv 3$ (mod 4), then $p$ is irreducible in $\mathbb{Z}[i]$.*

*Proof.* Let $p \in \mathbb{N}$ be prime in $\mathbb{Z}$, and assume $p \equiv 3 \pmod 4$, but $p = (a+bi)(c+di)$, for some non-units $a+bi$ and $c+di$. Then taking the norm,

$$\begin{aligned} N(p) &= N[(a+bi)(c+di)] \\ p^2 &= N(a+bi)N(c+di) \\ p \cdot p &= (a^2+b^2)(c^2+d^2). \end{aligned}$$

Then we have $a^2 + b^2 = p \quad$ and $\quad c^2 + d^2 = p$.

Let us consider the equation $a^2 + b^2 = p$. Since $p \equiv 3 \pmod 4$ , we have

$$a^2 + b^2 \equiv 3 \pmod 4.$$

By proposition 5.3.1 this is impossible since the only possible answer is $a^2+b^2 \equiv 0, 1 \pmod 4$. Therefore if $p = (a + bi)(c + di)$, then either $a + bi$ or $c + di$ is a unit. □

**Corollary 6.2.5.1.** *Let $p$ be an ordinary prime. If $p \equiv 3$ (mod $4$), then $p$ cannot be expressed as the sum of two squares in $\mathbb{N}$.*

*Proof.* The proof follows directly from the result that for some $a, b \in \mathbb{N}$, if

$$p = a^2 + b^2,$$

then $a^2 + b^2 \equiv 3 \pmod 4$ is impossible by the above theorem. □

We can use the factorization table again to confirm what we have discussed so far. The following Theorem generalizes the various types of Gaussian primes.

**Theorem 6.2.6.** *Let $a+bi$ be a Gaussian integer. The following is a categorisation of all possible Gaussian primes.*

- $N(a + bi) = p$, *for a prime* $p \in \mathbb{N}$ *with* $p = 2$, *or* $p \equiv 1$ *(mod* $4$*), and* $a, b \neq 0$.
- $a = 0$ *and* $b$ *is a prime in* $\mathbb{Z}$, *with* $|b| \equiv 3$ *(mod* $4$*).*
- $b = 0$, *and* $a$ *is a prime in* $\mathbb{Z}$, *with* $|a| \equiv 3$ *(mod* $4$*).*

# Chapter 7

# Application

## 7.1 General Application

We aim to apply all the results of previous chapters to the understanding of Pythagorean triples, and how they relate to Gaussian integers.

We first want to learn how to factorize Gaussian integers into Gaussian irreducibles using the theory we learnt throughout the paper.

**Example 15.** *Let $\alpha = 33 + 99i$ be a Gaussian integer. Suppose we can find an irreducible Gaussian integer $\gamma$ that divides $\alpha$. Since $\gamma$ is irreducible, if $\gamma|\alpha$, then $\gamma|\alpha\overline{\alpha} = N(\alpha)$. We first calculate and factor $N(\alpha)$:*

$$N(33 + 99i) = (33)^2 + (99)^2 = 10890 = 2 \cdot 3^2 \cdot 5 \cdot 11^2 \tag{7.1}$$

*Hence $\gamma|10890$. By Euclid's Lemma for Gaussian integers (Lemma 4.2.1), $\gamma|2$ or $\gamma|3$ or $\gamma|5$, or $\gamma|11$. We consult the factorization table for help. Up to order of units the table gives the following factorizations.*

$$2 = (1 + i)(1 - i), \quad 5 = (1 + 2i)(1 - 2i), \quad 11 = 1(11).$$

*We know by example 7 that the Gaussian integer 3 is irreducible in $\mathbb{Z}[i]$. If $\gamma|10890$ then $\gamma$ is a factor in one of these factorizations. We now attempt to find the true factorization of $\alpha$.*

*Choose elements $a, b, c, d, e, f$ in $\mathbb{Z}$, and $u \in U(\mathbb{Z}[i]$ such that,*

$$33 + 99i = u \cdot (1 + i)^a(1 - i)^b \cdot 3^c \cdot (1 + 2i)^d(1 - 2i)^e \cdot 11^f \tag{7.2}$$

*Taking the norm of this equation gives*

$$N(33+99i) = 1 \cdot 2^a \cdot 2^b \cdot 3^{2c} \cdot 5^d 5^e \cdot 11^{2f} = 2^{a+b} \cdot 3^{2c} \cdot 5^{d+e} \cdot 11^{2f}. \quad (7.3)$$

*Matching equations* 7.1 *and* 7.3 *we get* $a+b=1, c=1, d+e=1, f=1$. *Substituting these values in equation* 7.2 *we get,*

$$\begin{aligned} 33+99i &= u \cdot (1+i)^a (1-i)^b \cdot 3^1 \cdot (1+2i)^d (1-2i)^e \cdot 11^1 \\ &= u \cdot (1+i)^a (1-i)^b \cdot (1+2i)^d (1-2i)^e \cdot 3 \cdot 11 \\ \frac{33+99i}{3 \cdot 11} &= u \cdot (1+i)^a (1-i)^b \cdot (1+2i)^d (1-2i)^e \\ 1+3i &= u \cdot (1+i)^a (1-i)^b \cdot (1+2i)^d (1-2i)^e. \end{aligned}$$

*Looking at the equation* $a+b=1$, *we have two options. Either* $a=0$ *and* $b=1$ *or* $b=0$ *and* $a=1$. *We start with the former.*
***a=0,b=1***.

$$\begin{aligned} 1+3i &= u \cdot (1+i)^0 (1-i)^1 \cdot (1+2i)^d (1-2i)^e \\ &= u(1-i) \cdot (1+2i)^d (1-2i)^e \\ \frac{1+3i}{1-i} &= u \cdot (1+2i)^d (1-2i)^e \\ -1+2i &= u \cdot (1+2i)^d (1-2i)^e. \end{aligned}$$

*Now we bring in the equation* $d+e=1$. *The options are* $d=1$ *and* $e=0$, *or* $d=0$ *and* $e=1$. *Let us consider the latter.*
$d=1, e=0$.

$$\begin{aligned} -1+2i &= u \cdot (1+2i)^0 (1-2i)^1 \\ &= u \cdot (1+2i) \\ \frac{-1+2i}{1+2i} &= \frac{3}{5} + \frac{4}{5} = u. \end{aligned}$$

*This is a contradiction since* $u \in U(\mathbb{Z}[i])$. *We check the other option.*
$d=0, e=1$.

$$\begin{aligned} -1+2i &= u \cdot (1+2i)^0 (1-2i)^1 \\ &= u \cdot (1-2i) \\ \frac{-1+2i}{1-2i} &= -1 = u. \end{aligned}$$

*Hence we have* $u = -1, a = 0, b = 1, c = 1, d = 0, e = 1, f = 1$ *which we substitute into equation* 7.2 *to get,*

$$\begin{aligned} 33 + 99i &= (-1) \cdot (1+i)^0(1-i)^1 \cdot 3^1 \cdot (1+2i)^0(1-2i)^1 \cdot 11^1 \\ &= (-1)(1-i) \cdot 3 \cdot (1-2i) \cdot 11. \end{aligned}$$

*Out of curiosity, for the equation* $a + b = 1$*, we consider the last option to see what the answer will look like.*
***a=1,b=0***.

$$\begin{aligned} 1 + 3i &= u \cdot (1+i)^1(1-i)^0 \cdot (1+2i)^d(1-2i)^e \\ &= u(1+i) \cdot (1+2i)^d(1-2i)^e \\ \frac{1+3i}{1+i} &= u \cdot (1+2i)^d(1-2i)^e \\ 2 + i &= u \cdot (1+2i)^d(1-2i)^e. \end{aligned}$$

*We bring in the equation* $d + e = 1$ *again. The options are* $d = 1$ *and* $e = 0$*, or* $d = 0$ *and* $e = 1$*. Let us consider the former.*
$d = 1, e = 0$.

$$\begin{aligned} 2 + i &= u \cdot (1+2i)^1(1-2i)^0 \\ &= u \cdot (1+2i) \\ \frac{2+i}{1+2i} &= \frac{4}{5} - \frac{3}{5} = u \end{aligned}$$

*a contradiction again since* $u \in U(\mathbb{Z}[i])$*. We consider the final option.*
$d = 0, e = 1$.

$$\begin{aligned} 2 + i &= u \cdot (1+2i)^0(1-2i)^1 \\ &= u \cdot (1+2i) \\ \frac{2+i}{1-2i} &= i = u. \end{aligned}$$

*Hence our final options are* $u = i, a = 1, b = 0, c = 1, d = 0, e = 1, f = 1$*, and substituting these options into equation* 7.2 *we get,*

$$\begin{aligned} 33 + 99i &= (i) \cdot (1+i)^1(1-i)^0 \cdot 3^1 \cdot (1+2i)^0(1-2i)^1 \cdot 11^1 \\ &= (i)(1+i) \cdot 3 \cdot (1-2i) \cdot 11. \end{aligned}$$

*We have two factorizations for* $33+99i$*, but since* $\mathbb{Z}[i]$ *is a UFD, the factorizations are the same with just a difference in their ordering up to units.*

*In this case the only options for* $\gamma$ *are* $1+i, 1-i, 1-2i, 3, 11$.

## 7.2 Pythagorean Triples

We use [9, 24] to gain insights on Pythagorean triples.

**Definition 7.2.1.** *Let* $x, y, z \in \mathbb{N}$*. The set* $(x, y, z)$ *is called a primitive Pythagorean triple if* $x^2 + y^2 = z^2$*, and* $gcd(x, y, z) = 1$ *in* $\mathbb{N}$*.*

We look at the parity of $x, y$ and $z$. By Conrad [9], $z$ cannot be even. We use proposition 5.3.1 to show why. If $z$ is even, and $x$ and $y$ are both even, then this contradicts the fact that $x, y, z$ are primitive Pythagorean triples. If $z$ is even, then both $x$ and $y$ are odd. By the second item of proposition 5.3.1, $z$ is not a square. Therefore $z$ is odd, and by the proposition, $x$ is odd and $y$ is even. For the next part we use Kahn [15] to guide us into proving that two Gaussian integers $x + iy$ and $x - iy$ are relatively prime in $\mathbb{Z}[i]$. We first give the following statement.

**Proposition 7.2.1.** *Let* $\alpha$ *be a Gaussian integer. The norm of* $\alpha$ *is even if and only* $\alpha$ *is a multiple of* $1 + i$*.*

The proof can be found on Conrad [9, p.30].

**Lemma 7.2.1.** *Let* $(x, y, z)$ *be a primitive Pythagorean triple. The Gaussian integer* $x + yi$ *and it's conjugate* $x - yi$ *are relatively prime in* $\mathbb{Z}[i]$*.*

*Proof.* We begin by writing the equation $x^2 + y^2 = z^2$ as,

$$(x + yi)(x - yi) = z \cdot z \tag{7.4}$$

To reiterate, $x$ is odd, $y$ is even, and $z$ is odd, which implies that $gcd(x, y) = 1$. To show that $x + yi$ and $x - yi$ are relatively prime in $\mathbb{Z}[i]$, we will prove that the only common divisor of the two Gaussian integers is a unit. Let $\gamma$ be a common divisor of $a + bi$ and $a - bi$. Then $\gamma | x + yi$ and $\gamma | x - yi$, and by proposition 3.1.1,

$$\gamma | (x + yi) + (x - yi) = 2x$$
$$\gamma | (x + yi) - (x - yi) = 2yi.$$

For the second case where $\gamma|(x+yi)-(x-yi)=2yi$, we can remove $i$ since it is a unit and remain with $\gamma|2y$. We then show that $\gamma$ is relatively prime to 2 in the ring $\mathbb{Z}[i]$. Form the factorization table, we have $2=(1+i)(1-i)$, but we can also write $2=-i(1+i)^2$. By Theorem 6.1.1, the integer $1+i$ is prime in $\mathbb{Z}[i]$. Therefore, to prove that $\gamma$ and 2 are relatively prime in $\mathbb{Z}[i]$, we have to show that $1+i$ does not divide $\gamma$. By Proposition 7.2.1, $(1+i)|\gamma$ if and only $N(\gamma)$ is even. We then want to show the parity of $N(\gamma)$. By Equation 7.4, $\gamma^2|z^2$, taking the norm, $N(\gamma^2)|N(z^2)$ which gives us $N(\gamma^2)|z^4$. Since $z$ is odd, $z^4$ is odd, which means $N(\gamma^2)$ is odd. Therefore $1+i\nmid\gamma$, and $\gamma$ and 2 are relatively prime in $\mathbb{Z}[i]$, which implies that $\gamma|x$, and $\gamma|y$.

Since $x$ and $y$ are relatively prime in $\mathbb{Z}$, they are also relatively prime in $\mathbb{Z}[i]$ [9, p.26]. Then, the common divisors of $x$ and $y$ in $\mathbb{Z}[i]$ are the units of $\mathbb{Z}[i]$. Therefore, $\gamma$ is a unit, and $x+yi$ and $x-yi$ are relatively prime in $\mathbb{Z}[i]$ as desired. □

**Theorem 7.2.2.** *Let $(x,y,z)$ be a Pythagorean triple. We can express $x,y,z$ as $x=u^2-v^2, y=2uv$, and $z=u^2+v^2$, for some $u$ and $v$ in $\mathbb{N}$.*

*Proof.* We begin with equation 7.4. By Lemma 7.2.1, the Gaussian integers $x+yi$ and $x-yi$ are relatively prime in $\mathbb{Z}[i]$. Since the product $z^2$ of these two Gaussian integers is a square, we can use the unique factorization of $\mathbb{Z}[i]$ to show that $x+yi$ is a square up to multiplication by units, and $x-yi$ is also a square up to multiplication by units. Note that this is true only up to multiplication by units. For example, we have

$$(-4)(-9)=(36).$$

In this case, $-4$ and $-9$ are relatively prime in $\mathbb{Z}$ ,and neither is a square, but their product is a square. Therefore considering the units of $\mathbb{Z}[i]$, the unit (-1) is a perfect square since $(i)^2=-1$. Therefore we can absorb it into any square when we write it as $i^2$. Let $u+vi$ be a Gaussian integer. Our Options for $x+yi$ are,

$$x+yi=(u+vi)^2 \text{ or } x+yi=i(u+vi)^2.$$

We expand the first equation to get, $x+yi=u^2+2uvi-v^2$. Equating coefficients gives us,

$$x=u^2-v^2 \text{ and } y=2uv.$$

We expand the second equation to get, $x+yi=i(u^2+2uvi-v^2)=-2uv+(u^2-v^2)$. Equating coefficients gives us,

$$x = -2uv \text{ and } y = u^2 - v^2.$$

We refer to our earlier statement that $x$ is even and $y$ is odd. As a result, the second expanding which gives us $x = -2uv$ and $y = u^2 - v^2$ cannot be true since it implies that $x$ is even. Therefore we take the second expansion. Since $(x, y, z)$ is a Pythagorean triple, we have $x^2 + y^2 = z^2$. Therefore,

$$x^2 + y^2 = (x + yi)(x - yi) = (u^2 + v^2)^2$$

$\therefore$ If $x^2 + y^2 = (u^2 + v^2)^2 = z^2$, we have $z = u^2 + v^2$.

□

We want to apply the theory of Pythagorean triples to cubes using Section 7.2 and Ho [13].

**Example 16.** *Solve for $x$ and $z$ in the equation $x^2 + 1^2 = z^3$, for some $x, z$ in $\mathbb{Z}$ using concepts from the Pythagorean triples.*

***Solution***

*We first study the parity of $x$ and $z$. If $x$ is odd, then as we have shown in Section 7.2, $x^2 \equiv 1$ (mod 4). This means that $x^2 + 1$ is divisible by 2, but it is not divisible by 4. But if $x$ is odd then $z$ has to be even. Hence if $z$ is even, then $z^3 = x^2 + 1^2$ is divisible by 8, which is a contradiction. This implies that $x$ is even, and $z$ is odd. The second part of the solution is to show that for $z^3 = x^2 + 1 = (x + i)(x - i)$, $x + i$ and $x - i$ are relatively prime in $\mathbb{Z}[i]$. We use the same methodology as with Pythagorean triples. Let $\gamma$ be a common divisor of $x + i$, and $x - i$, then*

$$\gamma | (x + i) - (x - i) = 2i.$$

*This means that either $\gamma = 1 + i$, or $\gamma = 1 - i$. However, since $\gamma | z$, by Proposition 3.2.1 we can then deduce that $2|z$, which is a contradiction. Therefore the Gaussian integers $x + i$ and $x - i$ are relatively prime in $\mathbb{Z}[i]$. As with the equation $(x + yi)(x - yi) = z^2$, we use the unique factorization property of Gaussian integers to state that, both $x + i$ and $x - i$ are Gaussian integer cubes up to multiplication by units. Notice that for the Gaussian integer units we have,*

$$(1)^3 = 1$$
$$(-1)^3 = -1$$
$$(i)^3 = -i$$
$$(-i)^3 = i.$$

*Then by the unique factorization of Gaussian integers,* $x + i$ *and* $x - i$ *can be written as Gaussian integers cubes up to units. Therefore,*

$$(x + i) = (u + vi)^3, \textit{ for some Gaussian integer } u + vi.$$

*Expanding the equation gives us,*

$$x + i = u^3 + 3u^2vi - 3uv^2 - v^3i \tag{7.5}$$

*Equating the imaginary coefficients gives us,*

$$1 = 3u^2v - v^3 \tag{7.6}$$

*We then solve equation* 7.6 *to get* $v(3u^2 - v^2) = 1$. *Therefore* $|v| = 1$ *and,*

$$\begin{aligned} 1 &= |3u^2 - (v)^2| \\ &= |3u^2 - (1)^2| \end{aligned}$$
.

*For this equation to hold, we must have* $u = 0$. *We substitute* $u = 0$ *in equation* 7.6, *to get* $3u^2v - v^3 = v[3(0)v^2 - v^2] = -v^3 = 1$. *Therefore* $v = -1$. *We then substitute both* $u$ *and* $v$ *equation* 7.5 *to get,*

$$x + i = (u + vi)^3 = (0) + (-1)i]^3 = (-i)^3 = i.$$

*Therefore* $x + i = i$, *which implies that* $x = 0$. *Substituting* $x$ *in the equation* $x^2 + 1^2 = z^3$, *we get* $(0)^2 + 1^2 = z^3$, *which implies that* $z = 1$.

$\therefore$ *The solution to the equation* $x^2 + 1^2 = z^3$ *is* $x = 0$, *and* $z = 1$.

# Chapter 8

# Conclusion

In general to simplify expressions of the form $x^2 - dy^2$ , we just have to factor the expression into it's linear factors

$$(x + y\sqrt{d})(x - y\sqrt{d}),$$

and work in the ring $\mathbb{Z}[\sqrt{d}]$, where $d$ is a square-free integer, and $d \equiv 2, 3 \pmod 4$. We then use the map $\varphi : \mathbb{Z} + \mathbb{Z}[\sqrt{d}] \to \mathbb{N} \cup \{0\}$ defined by ,

$$\varphi(x + y\sqrt{d}) = |x^2 - dy^2| \in \mathbb{N} \cup \{0\},$$

to prove that this set of quadratic rings is a Euclidean domain, so that we can apply the appropriate properties. This approach is very useful in solving equations like Pell's equation which is defined by

$$x^2 - dy^2 = 1, \text{ for some } x, y \in \mathbb{Z}.$$

According to sequence A048981 of Sloane [23], the values of $d \equiv 2, 3 \pmod 4$ for which the ring $\mathbb{Z}[\sqrt{d}]$ is Euclidean with respect to the map $\varphi$ are,

$$d = -1, -2, 2, -3, 3, 5, 6, -7, 7, -11, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

It can be proven that every Euclidean domain is a principal ideal domain, but the converse is false. In fact, when

$$d = -19, -43, -67, -163,$$

the Euclidean domain $\mathbb{Z}[\sqrt{d}]$ is not a principal ideal domain. We can also prove that when a Euclidean domain is a principal ideal domain, then it is also unique factorization domain. In fact by Muthukumar [19], $\mathbb{Z}[\sqrt{d}]$ is a UFD when

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

These numbers are called Heegner numbers. It is important to note that all the Euclidean domains as per Sloane [23] made it to the list of UFDs, which proves our claim that every Euclidean domain is a principal ideal domain.

Therefore, when dealing with quadratic rings, all one needs to do is check whether their quadratic ring of focus is a Euclidean domain from the list above. Other key concepts will follow from this discovery alone, saving us time and resources so that we can focus on the important concepts that are yet to be proven.

Gaussian integers are truly a remarkable form of integers with properties that are not only thought provoking, but also fundamental to our understanding of key concepts in both number theory and algebra, and even in other fields of mathematics. We can apply the theory of Gaussian integers to many more concepts across various fields in Mathematics. For example, in solving the Pythagorean equation $x^2 + y^2 = r$ which is just looking for the Gaussian primes $p$ such that $p \equiv 1 \pmod 4$, and letting $p = r$. We can also use Gaussian integers to understand integers of the form

$$(1 \pm i)^n - 1,$$

which are called Gaussian Mersenne integers, and called Gaussian Mersenne primes when $n = p$, for a prime $p \in \mathbb{N}$. We can use these integers to understand Mersenne numbers in $\mathbb{Z}$, and many more. The possibilities are just endless.

To close the project, we have to admit that the journey towards learning about Gaussian integers has been a truly eye-opening one because not only has it introduced us to new concepts, it has also helped us properly understand the most fundamental concepts of Mathematics that we may have thought of as too trivial, while in truth, how they are formulated and how they can be utilized is anything but trivial.

# Bibliography


[1] Şaban Alaca and Kenneth S Williams. *Introductory algebraic number theory*. Cambridge University Press Cambridge, 2004.

[2] Michael Artin. *Algebra*. Prentice-Hall, Inc, 1991.

[3] Shreejit Bandyopadhay. Euclidean domains and the gaussian integers:an application. *https://www.cmi.ac.in/~shreejit/Gaussian.pdf*, 2013. Accessed on 08 January 2020.

[4] Eric Temple Bell. *Men of mathematics*. Simon and Schuster, 2014.

[5] Lee A Butler. A classification of gaussian primes. *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.568.1607&rep=rep1&type=pdf* , 2019. Accessed on April 2019.

[6] Jack S Calcut. Gaussian integers and arctangent identities for $\pi$. *The American Mathematical Monthly*, 116(6):515–530, 2009.

[7] Pete L Clark. The gaussian integers i: The fundamental theorem. *https://pdfcoffee.com/qdownload/gaussian-intergers-zi-pdf-free.html*, 2017. Accessed on April 2019.

[8] Keith Conrad. Remarks about euclidean domains. *https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf*, 1991. Accessed on 19 February 2020.

[9] Keith Conrad. The gaussian integers. *https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf*, 2008. Accessed on 03 January 2019.

[10] Greg Dresden and Wayne M Dymàček. Finding factors of factor rings over the gaussian integers. *The American Mathematical Monthly*, 112(7):602–611, 2005.

[11] John B Fraleigh. *A first course in abstract algebra*. Pearson Education India, 2003.

[12] Godfrey Harold Hardy, Edward Maitland Wright, et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

[13] Ho Hung. Gaussian integers. *Available online at the URL,* `http://math.uchicago.edu/~may/REU2016/REUPapers/Ho.pdf`, 2019. Accessed on 25 January 2019.

[14] Thomas W Judson. *Abstract algebra: theory and applications*. Austin State University, 1997.

[15] PETER J Kahn. Trisection, pythagorean angles, and gaussian integers. *http://pi.math.cornell.edu/ kahn/pythagoreantrisection.pdf*, 2011. Accessed on 12 February 2019.

[16] Israel Kleiner. From numbers to rings: The early history of ring theory. *Elemente der Mathematik*, 53(1):18–35, 1998.

[17] James S Milne. Algebraic number theory (v3.04). 2012. Available at `www.jmilne.org/math/`.

[18] M Ram Murty and Jody Esmonde. *Problems in algebraic number theory*, volume 190. Springer Science & Business Media, 2005.

[19] T Muthukumar. Complex prime numbers. `http://home.iitk.ac.in/~tmk/reachout/ComplexPrime.pdf`, 2014. Accessed on 16 July 2020.

[20] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[21] Kenneth H Rosen. *Elementary number theory*. Pearson Education, 2011.

[22] JJ Rotman. Advanced modern algebra, 2002. Prentice Hall, New York.

[23] Neil Sloane. The on-line encyclopedia of integer sequences. *http://oeis.org*, 2020. Accessed on 21 July 2020.

[24] John Stillwell. *Elements of number theory*. Springer Science & Business Media, 2002.

[25] Mak Trifković. *Algebraic theory of quadratic numbers*. Springer, 2013.